Digital Festning Europa

en studie av informasjonssamarbeidet i Schengenområdet, dets kontrollører og effekter.

Renate Wejset

Masteravhandling i Rettssosiologi

Institutt for Kriminologi og Rettssosiologi

Juridisk Fakultet

UNIVERSITETET I OSLO

Mai, 2013

"Nothing to hide, nothing to fear. If you have nothing to hide you must have lived a very boring life". – Statewatch.

Digital Festning Europa

en studie av informasjonssamarbeidet i Schengenområdet, dets kontrollører og effekter.

Renate Wejset

Masteravhandling i Rettssosiologi

Institutt for Kriminologi og Rettssosiologi

Juridisk Fakultet

UNIVERSITETET I OSLO

8.5.2013

Digital Festning Europa – en studie av informasjonssamarbeidet i Europa, dets kontrollører og effekter.

Institutt for Kriminologi og Rettssosiologi, Juridisk Fakultet, Universitetet i Oslo.

http://www.duo.uio.no/

Trykk: Allkopi.

Sammendrag

Tittel: Digital Festning Europa – en studie av informasjonssamarbeidet i Europa, dets kontrollører og effekter.

Av: Renate Wejset

Veileder: Thomas Mathiesen

Vår 2013, Universitetet i Oslo, Institutt for Kriminologi og Rettssosiologi.

Schengen-samarbeidet representerer et reisefrihetsområde mellom Schengen-landene og en «mur» mot utenforliggende land, fortrinnsvis med tanke på å bekjempe ulovlig innvandring til området. For å kompensere for reisefriheten Europas borgere besitter har man lagt opp til et omfattende internasjonalt politisamarbeid Schengen-landene i mellom som er gjenstand for avhandlingen. Schengen Informasjonssystem (SIS) er politiets hovedverktøy i samarbeidet der mengder av informasjon om personer og gjenstander lagres og utveksles mellom landene. Hovedsakelig skal systemet inneholde opplysninger om uønskede «inntrengere» til Schengen-området, og det omtales som et overvåkingssystem. SIS står ikke alene som verktøy i informasjonssamarbeidet, men er en del av et stort nettverk av systemer som totalt utgjør en svært omfattende overvåkings- og kontrollstruktur i Europa. Avhandlingen søker å risse ut et bilde av dette omfanget og gi leseren en forståelse av hvilken enorm overvåkingsstruktur vi står overfor.

Schengen-samarbeidet omfatter i 2013 26 land. Vi er med dette vitne til en globalisering av lover og regler innad i Europa som skaper en rekke utfordringer. Selv om reglene knyttet til Schengen skal gjelde for alle medlemsland vil landenes egne lover kunne føre til ulikhet i praksis og behandling av personopplysninger i SIS. I tillegg kan det være store forskjeller i praksis med hensyn til blant annet hvem som har tilgang i de ulike land og hvor sikret opplysningene generelt sett er. I dette henseendet reises en rekke spørsmål knyttet til individers rettssikkerhet og personvern som avhandlingen ser nærmere på.

Politiet driver overvåking, kontroll og lagring av informasjon om borgere både i Schengen-landene og land utenfor, men dette er ikke unndratt kontroll fra andre instanser. De kritiske røstene og «kontrollørenes kontrollører» i form av ulike tilsynsorganer og ikke-statlige organisasjoner (NGO's) spiller en rolle i maskineriet. Avhandlingen søker å se nærmere på

hvem disse kontrollørene og kritikerne er, og reiser spørsmålet i hvilken grad deres «overvåkende» øyne har en effekt, samt hva som påpekes av disse som kritikkverdig. «Det sivile blikket» som kontrollør kan også være avgjørende, og avhandlingen ser nærmere på hvordan kontrollen av et så lukket system som Schengen Informasjonssystem faktisk fungerer. Har man innsynsrett i opplysninger om en selv? Er befolkningen seg bevisst den omfattende overvåkingsstrukturen som har vokst frem i Europa? Dette vil berøre sentral rettssosiologisk teori; rettspluralisme, globalisering av lover og politiarbeid, teoretiseringen av «risikosamfunnet» og overvåking som fenomen.
Kripos som utøvende organ av SIS i Norge er en essensiell stemme i avhandlingen, der målet har vært å komme på innsiden av systemet i den grad det er mulig, for å slippe Kripos til med deres synspunkter. Innsiden og utøverne av SIS settes således opp mot systemets kritikere og kontrollører som betrakter systemet fra utsiden. Avhandlingen vil vise at ens ståsted, og dermed forståelseshorisont, i stor grad påvirker hvordan man betrakter systemet.
Avhandlingen baseres hovedsakelig på empirisk materiale skaffet til veie ved kvalitative intervjuer; totalt 9 informanter.

Avhandlingen viser at det fremdeles er en lang vei å gå med tanke på individers rettssikkerhet og personvern i SIS. Muligens vil faremomentene systemene representerer eskalere etter hvert som informasjonssystemene, deriblant SIS utvikler seg.

Det blir sett nærmere på de effekter Schengen-samarbeidet har hatt i forhold til målsettingene, og spørsmålet reises om utviklingen har tatt en annen retning enn ønskelig. Avhandlingen skisserer og drøfter således et par mulige alternativer for Norge og «Schengenveien» videre.

Forord

En teoretisk rundreise i Schengenområdet er over, og det er på tide å takke mitt reisefølge.

Først og fremst vil jeg takke min veileder Professor Thomas Mathiesen. Takk for at du har øst av din kunnskapsbrønn, kommet med nyttige innspill og engasjert deg i morsomme og interessante samtaler med meg på sene ettermiddager. Du hadde rett; siste ord er ikke sagt!

Jeg vil også takke Vidar Halvorsen som med sitt sylskarpe blikk og ikke minst penn har veiledet oss på gruppebasis. Uten deg ville vi stått mye alene.

Tusen takk til alle de interessante og kunnskapsrike menneskene jeg har møtt – mine informanter. Jeg er evig takknemlig for at dere ryddet tid i deres pressede tidsplaner og at jeg fikk møte dere alle og en.

Jeg vil takke mitt arbeidssted Ipsos MMI v/Karin Bjørnstad som har gitt meg tid til å følge undervisning og har utvist stor forståelse og engasjement rundt mitt arbeid med avhandlingen. Jeg vil takke mine gode kolleger, spesielt Tonje, som har hørt på mine små og store frustrasjoner og kommet med gode råd. Tusen takk.

Jeg vil takke de fantastiske studiekameratene som har gjort studietiden og arbeidet mye lettere. Jeg er uendelig glad for at jeg traff dere! Skulle ønske jeg kunne få vært mer sammen med dere på skolen. Og ikke minst mine gode gamle venner for god støtte og oppmuntrende ord. Takk til Pappa som har tro på meg uansett hva jeg holder på med. Tusen takk til Marianne Moen som var villig til å korrekturlese avhandlingen.

Jeg må igjen takke deg Thomas for at du gjorde meg interessert i tematikken rundt Schengen-samarbeidet.

Renate Wejset

Oslo, mai 2013.

Innholdsfortegnelse

1 Innledende ord

Det å berøre ved EU og dets enorme maskineri gjør at en til tider kan føle seg ganske liten. Selv om man kun vandrer i en liten del av EU-jungelen, i justisdelen, er det utfordrende å orientere seg i et vell av systemer, organer, dokumenter og personer som alle har sin rolle og oppgave i systemet. Etter hvert som man vandrer dukker nye spørsmål opp, nye paralleller dras, og man befinner seg i et finmasket nett av regler, organer og foranstaltninger som er mer komplekst enn man kunne forestille seg på forhånd. Feltet er også høyst levende; kartet man skaffet seg i går behøver ikke passe til dagens terreng. Veien blir til etter hvert som man går, og systemet er så omfattende at det kjennes som vandringen ikke noen gang behøver å ta slutt.

Temaet for min avhandling er Schengen-samarbeidet. Men også dette temaet representerer så mye mer enn man først tenker seg.
Schengen-samarbeidet representerer mer enn en streng kontroll av Schengenområdets yttergrenser og reisefrihet for Europas borgere innad. Samarbeidet representerer også et lite kjent og svært omfattende politisamarbeid mellom medlemslandene som vil være gjenstand for avhandlingen. Politisamarbeidet og informasjonsutvekslingen utføres i all hovedsak via politiets eget system; Schengen Informasjonssystem (SIS). I dette systemet lagres og utveksles en rekke opplysninger mellom Schengenlandene om personer og gjenstander av ulike årsaker, men fortrinnsvis uønskede personer fra tredjeland til Schengenområdet. SIS omtales svært ofte som et overvåkingssystem.

Dette omfattende instrumentet for informasjonsutveksling har ført til at en rekke spørsmål om individers personvern og rettssikkerhet reises. Disse spørsmålene har fulgt systemet gjennom hele dets eksistens, men avtar likevel ikke i aktualitet. Det vil muligens medføre riktighet å si at det tiltar.

I mitt arbeid har jeg hatt et ønske om å sette «innsiden» og brukerne av systemet opp mot «utsiden» av systemet. Innsiden representeres ved Politiet, for Norges del Kripos. «Utsiden» representeres ved systemets kritikere og tilsynsmyndigheter. Hva vil ens ståsted ha å si for hvordan en vurderer systemet?
Politiet driver økt grad av overvåking, men er samfunnet blitt så farlig at dette er nødvendig, eller er det de teknologiske nyvinninger som gjør det mulig å finjustere vårt overvåkende blikk? Kan overvåkingen i seg selv bringe med seg noen faremomenter?

Når man skal studere et felt som Schengen-samarbeidet der mange land inngår, vil man krysse mange ulike tematiske problemstillinger på veien. Man vil måtte betrakte de fenomener som oppstår ved at man har globalisering som en sentral ingrediens, og de virkninger dette kan ha er ikke få. Lover og regelverk er ikke lengre forbeholdt den enkelte nasjonalstat, men spres over grensene og begynner å gjelde flere steder. Hva skjer når retten globaliseres, og hvilke effekter har dette?

For å forstå og finne ut av hvordan samarbeidet og informasjonssystemet fungerer, samt se på hvilke effekter som oppstår i kjølvannet av systemene, har jeg kontaktet personer som enten via sitt daglige virke eller i kraft av sitt interesseområde kan bidra med informasjon. Avhandlingen vil således hovedsakelig basere seg på kvalitative intervjuer.

Arbeidet med avhandlingen har vist meg først og fremst at temaene som tas opp veves inn i et uløselig nett som har sterke paralleller ut i samfunnet på flere områder. Temaene jeg vil berøre stopper ikke på den tematiske grensen mot Schengen, men har ringvirkninger ut i samfunnet og inn i rettssystemet, også på et internasjonalt nivå på et langt større plan enn jeg i utgangspunktet var klar over. Dette berører et av de mest elementære temaene innenfor rettssosiologisk teori; vekselvirkningen mellom rett og samfunn (Mathiesen, 2005).

1.1 Problemstilling og avgrensning

Politisamarbeidet i Europa er svært omfattende og består etter hvert av et nettverk av systemer og samarbeidspartnere. Avhandlingen vil kretse rundt det største og mest omfattende systemet som benyttes av politiet i Europa i dag; Schengen Informasjonssystem (SIS). Mitt hovedspørsmål er i hvilken grad internasjonal overvåking ved SIS er en trussel for individers rettssikkerhet og personvern, og hvilke motkrefter som finnes til dette. Jeg kommer til å ønske å se nærmere på hvem som overvåker overvåkerne, og hva som påpekes av disse som utfordringer. Jeg ønsker å se på hva som var hensikten med Schengen-samarbeidet, og om man har oppnådd målsettingene. Har man også fått som resultat utilsiktede virkninger? Jeg kommer også til å skissere et par mulige scenarier for Norges del og «Schengenveien» videre.

Norge er del av et stort maskineri som medlem av Schengen, samtidig som vi ikke er medlem av EU. I hvilken grad står Norge i en avmaktsposisjon til systemet vi nå er en del av? Har Norge mistet en del av sin selvråderett?

Jeg vil underveis i avhandlingen berøre mange systemer og organer som er, og ser ut til å ville bli tett sammenvevet med dagens SIS. Disse vil ikke i uttømmende grad bli gått i gjennom, da dette kun er til det formål å bidra til å svare på mine problemstillinger. Da SIS er et system som kun benyttes innenfor Schengenlandene vil den tematiske avgrensningen også følge Schengens grenser, selv om dette vil sees i lys av et globalt perspektiv.

Overvåking gjennomsyrer hele vår eksistens, men dette som fenomen vil ikke bli berørt i sin helhet, og vil kun dreie seg rundt Schengen Informasjonssystem.

1.3 Tidligere arbeider på feltet

Størsteparten av litteratur og arbeid knyttet til Schengen-samarbeidet er utført av Professor Thomas Mathiesen ved Universitet i Oslo, Juridisk fakultet. Tidligere student ved Institutt for Kriminologi og Rettssosiologi Simen Wiig behandlet temaet i sin masteravhandling fra 2007; «*Flyt og tilgjengelighet: en studie av det europeiske informasjonssamarbeidet innen politi-, sikkerhets- og grensekontroll og dets konsekvenser for individers rettssikkerhet og rettigheter*» der han i imponerende grad blant annet tok for seg de tekniske sidene ved Schengen Informasjonssystem. Wiig forsøkte i sin tid å oppnå kontakt med Kripos som databehandler i Norge, uten den gang å få respons fra Kripos.

Stephen Kabera Karanjas doktoravhandling fra 2008 må også nevnes: "*Transparency and Proportionality in the Schengen Information System and Border Control Co-Operation".*

Min tilnærming skiller seg fra de overnevnte da det er systemets kontrollører og kritikere som vil stå i fokus for avhandlingen.

2 Et grenseløst samarbeid

Schengen-samarbeidet er et komplekst system. Før jeg detaljert presenterer mitt prosjekt vil jeg fremstille Schengen-samarbeidet og plassere dette i en teoretisk ramme.

Schengenområdet kan sammenliknes med Norden; et landområde der innbyggerne kan reise fritt uten grensekontroll (Kvam, 2008). Ønsket om å bevare den nordiske passunionen – «Det nordiske reisefrihetsområdet» - var en stor del av årsaken til at Norge ønsket å bli med i Schengen-samarbeidet (Kvam, 2008). Avtalen ble i første omgang inngått mellom Frankrike, Tyskland og Benelux-landene (Belgia, Nederland og Luxembourg) i 1985 (Mathiesen, 2000). Flere og flere land har kommet med i samarbeidet og medlemskap er nå så å si regelen snarere enn unntaket i Europa. Norge ble tilsluttet samarbeidet i 2001. I 2013 har Schengenområdet 26 medlemsland, og dekker 400 millioner mennesker (Mathiesen, 2013).

Hovedformålet med samarbeidet er å holde uønskede inntrengere ute fra dette store landområdet, særskilt personer fra den 3. verden, mens borgere innenfor grensene kan reise enkelt og passfritt (Mathiesen, 2000). Det går et tydelig skille mellom land innenfor Schengen og land utenfor. Alle personer som eksempelvis ønsker å besøke Norge fra et ikke-Schengenland må ha et besøks-visum som gir mulighet for å oppholde seg i Norge i inntil 90 dager (udi.no 2.3.2013). Man kan likevel som borger i et EU/EØS/EFTA-land, eksempelvis borgere fra Bulgaria og Romania besøke Norge uten å ha oppholdstillatelse. I tillegg har Norge avtale om visumfrihet med en rekke andre stater spredt over hele verden (udi.no 2.3.2013). Tilfredsstiller man de overnevnte krav vil terskelen til å reise inn i, eller gjennom et Schengenland være lav og man kan reise enklere enn tidligere.

Norge var i utgangspunktet noe tilbakeholden med å gå inn i Schengen-samarbeidet (Kvam, 2008). Avtalen kunne stride mot Grunnloven og dessuten hadde Norges borgere stemt nei mot EU. Man overveiet også det faktum at Norge ville få mindre selvbestemmelsesrett i asyl- og flyktningpolitikk, samtidig som personer på flukt kunne få et dårligere vern. Det var også generelle spørsmål rundt personvern og rettssikkerhet som reiste seg (Kvam, 2008).

Men avtalen representerer mer enn enklere reiser med færre papirer (Mathiesen, 2000). De fleste vil forbinde Schengen-avtalen med passfriheten mellom landene, men er seg nok ikke bevisst det omfattende politi- og overvåkingssamarbeidet landene i mellom. Flere ankepunkter reiser seg i dette henseendet.

2.1 Schengen-samarbeidet i praksis

Man har bygget ned den indre grensekontrollen landene i mellom, og opp den ytre grensekontrollen på landenes yttergrenser (Mathiesen, 2000). Hvert land har ansvaret for sin egen yttergrense til tredjeland og dersom man blir nektet adgang til *ett* Schengenland blir man nektet adgang til *alle*. Man snakker derfor gjerne om *Festning Europa*. Et viktig formål er altså en felles utestengningspolitikk fra landene som ligger utenfor Schengenområdet (Mathiesen, 1997). Schengen ble fremstilt som et tiltak for økt grad av frihet der man kunne reise passfritt i Europa og skulle samtidig være bekjempende mot kriminalitet (Mathiesen, 1997). Det blir likevel ofte hevdet at hovedformålet med Schengen-samarbeidet først og fremst er utestenging av uønskede, ikke nødvendigvis kriminalitetsbekjempelse (Mathiesen, 1997). For å kunne bevokte yttergrensene på en effektiv måte opprettet EU i 2004 et eget organ som bevokter og koordinerer dette arbeidet; FRONTEX (frontex.europa.eu 10.3.2013). På verdensbasis generelt må man kunne si at det er fokuset på organisert kriminalitet og terrorisme som har gjort at politiarbeidet har ekspandert utover landegrensene (Bowling og Sheptycki, 2012).

For å *kompensere* for nedbyggingen av grensekontrollen på de indre grensene har man lagt opp til økt grad av *overvåking* og *politisamarbeid* landene i mellom (Kvam, 2008). Norges representant og operative enhet i dette samarbeidet er Kripos ved SIRENE-kontoret. Politisamarbeidet har ført med seg omfattende strukturer med *overvåkingssystemer* og *registreringssystemer* som fører til enorme muligheter for informasjonsutveksling over landegrensene (Mathisen, 2000). Vi har på denne måten vært vitne til en akselererende utvikling på vei inn i en ny dimensjon av overvåking. Schengen-samarbeidet kan også sees på som et laboratorium for EU der justissamarbeidets nye ordninger prøves ut (Mathiesen, 2000).

En faktor som gjør at overvåking og politiarbeid lar seg utvikle og globalisere i den størrelsesorden vi i dag er vitne til er den teknologiske utviklingen. Denne gjør det mulig ved et tastetrykk å flytte mengder av informasjon til andre siden av jordkloden på under en brøkdel av et sekund. Det er nærliggende å anta at man i større grad har tatt i bruk ”føre-var” prinsippet der man ved utstrakt bruk av overvåking og samarbeid forsøker å sikre seg mot det som en dag måtte komme.

2.2 Kompenserende tiltak

Når man har bygget ned grensekontrollen har man måttet kompensere for dette. De kompenserende tiltakene man har tatt i bruk manifesterer seg i det digitale politisamarbeidet på kryss av landegrensene i Europa (Mathiesen, 2000). Kontrollen er ikke lengre synlig i form av en grensevakt, men har blitt skjult og fått en digital karakter. Spaningsfellesskapet er bygget opp, datasamarbeidet har økt, og det *generelle kontrollvolumet* har dermed gått opp. For å kunne oppfylle målet med å kontrollere grensene har politiet i Schengenlandene i utgangspunktet to systemer der man kan utveksle informasjon; SIS og SIRENE (Mathiesen, 2000). Disse systemene vil altså ikke stå for det operative politiarbeidet som arrestasjoner og liknende, men vil bidra, forme og tilrettelegge gjennom å samle, formidle og lagre informasjon (Loader, 2002).

Spesielt i tiden etter terrorangrepet i New York i 2001 har man i større og større grad tatt i bruk biometriske data i kampen mot terror og kriminalitet, og dette blir sett på som avgjørende for å opprettholde sikkerheten (Fierke, 2007). Man legger blant annet inn biometriske data i reisedokumentasjon som pass, og her har vi nok bare sett begynnelsen. All digitalisert biometrisk data og persondata betegnes av Dillon (2003) som «*virtuell sikkerhet*» (Dillon i Fierke, 2007). Alt og alle blir betraktet som en potensiell fare eller trussel. Som vil bli vist senere er biometriske data og utveksling av denne i gang i stor utstrekning i Europa.

Selv om det er en oppfatning blant mange at det var først ved terrorangrepet på New York at det hele startet, er det viktig å være klar over at utviklingen med hensyn til overvåking har startet lenge før dette (Mathiesen, 2013). De ulike informasjons- og overvåkingssystemene er et bevis på dette. Det er tre mål som er til felles for de ulike systemene; *bekjempelse av terror*, *bekjempelse av organisert kriminalitet* og *kontroll av EU's yttergrenser* (Mathiesen, 2013).

2.2.1 SIS (Schengen Informasjonssystem)

Kommunikasjonen og samarbeidet mellom politienhetene foregår først og fremst gjennom utveksling av informasjon i Schengen Informasjonssystem (SIS) som er det største systemet av sin sort i Europa. Systemet ble lansert i 1995, og majoriteten av opplysningene i SIS er knyttet til personer fra tredjeland (Brouwer, 2008).

SIS inneholder standardiserte faktaopplysninger om personer, savnede kjøretøy og objekter (Mathiesen, 2000). SIS har en sentral database i Strasbourg og alle medlemslandene har sine egne nasjonale databaser knyttet opp mot denne (Mathiesen, 2000). I tillegg benyttes SIRENE som på sin side inneholder "myke" tilleggsopplysninger til SIS i fritekst.

Formålet med SIS beskrives i Schengenkonvensjonen:

> *"The purpose of the Schengen Information System shall be in accordance with this Convention to maintain public policy and public security, including national security, in the territories of the Contracting Parties and to apply the provisions of this Convention relating to the movement of persons in those territories, using information communicated via this system".* (Schengenkonvensjonen, 2007, art.93).[1]

Man kan bli registrert i SIS av ulike årsaker og disse står definert i Schengenkonvensjonen. Man skal gjøre en vurdering i hvert enkelt tilfelle basert på om det foreligger en sikkerhetsmessig trussel ved å ha en gitt person på et landområde (Schengenkonvensjonen 2007 art.96). Dette gjelder spesielt i følgende tilfeller:

> *a) an alien who has been convicted of an offence carrying a penalty involving deprivation of liberty of at least one year;*
>
> *b) an alien in respect of whom there are serious grounds for believing that he has committed serious criminal offences, including those referred to in Article 71, or in respect of whom there is clear evidence of an intention to commit such offences in the territory of a Contracting Party.*
>
> *3) Decisions may also be based on the fact that the alien has been subject to measures involving deportation, refusal of entry or removal which have not been rescinded or suspended, including or accompanied by a prohibition on entry or, where applicable, a prohibition on residence, based on a failure to comply with national regulations on the entry or residence of aliens* (Schengenkonvensjonen 2007, art.96).

Man kan altså registreres i SIS selv om man foreløpig ikke har begått en kriminell handling, men dersom det foreligger en mistanke om at en slik handling kommer til å bli begått i fremtiden. Informasjon om vitner og personer som skal inn til rettssak eller soning kan også registreres slik at man kan holde kontroll på personers bosted (Schengenkonvensjonen, 2007 art.98). Man kan også registreres dersom det vurderes som sannsynlig at en person vil få tilbakefall basert på tidligere handlinger (Schengenkonvensjonen 2007, art.99). Det er

[1] Schengenkonvensjonen har utkommet i flere versjoner. I avhandlingen benyttes versjonen fra 2007 som ble sendt til meg fra en av mine kontakter i Kripos slik at jeg skulle slippe å navigere blant de ulike versjonene på egenhånd. Dette er årsaken til at det vil henvises til et årstall som er meget fjernt fra Schengen-samarbeidets fødeår; 1985.

nærliggende å anta at dersom man først har kommet på innsiden av SIS kan veien være lang og tung ut igjen. Det er riktignok *saneringsregler* i systemet, men dette må også overholdes i likhet med alt annet reglement. Dette vil bli tatt opp i mer utførlig grad senere.

I SIS kan følgende opplysninger om *person* registreres (hentet fra Schengenkonvensjonen, 2007 art.94):

a) *Surname and forenames, any aliases possibly entered separately*
b) *Any specific objective and physical characteristic not subject to change*
c) *First letter of second forename*
d) *Date and place of birth*
e) *Sex*
f) *Nationality*
g) *Whether the persons concerned are armed*
h) *Whether the persons concerned are violent*
i) *Reason for the alert*
j) *Action to be taken*

Man kan også registrere og kommunisere følgende tilleggsopplysninger (Schengenkonvensjonen, 2007 art.99).

a) *The fact that the person for whom or the vehicle for which an alert has been issued has been found;*
b) *The place, time or reason for the check;*
c) *The route and destination of the journey;*
d) *Persons accompanying the person concerned or occupants of the vehicle;*
e) *The vehicle used*
f) *Objects carried*
g) *The circumstances under which the person or the vehicle was found.*

Måten man skal opptre på understrekes i Schengenkonvensjonen: «*During the collection of this information steps must be taken not to jeopardize the discreet nature of the surveillance*» (Schengenkonvensjonen, 2007 art.99).

For å gi et innblikk i omfanget av opplysninger som står registrert i SIS viser jeg til statistikk som i januar 2013 ble publisert av Council of The European Union. Oversikten viser omfanget av de ulike registreringstypene slik systemet fremstår i dag. Tabellen til høyre viser ettersøkte personer fordelt på de ulike artikkeltypene (summert under «WP wanted persons» i tabellen til venstre).

Tabell 1:

Type	Number of Valid records (Not expired):
Banknotes	257 869
Blank Dokuments	697 097
Firearms	421 194
Issued Documents	38 901 431
Vehicles	5 071 806
WP (wanted persons)	885 807
WP (alias)	283 374
Total	46 518 578

Article of the Convention	Number of Valid records (Not expired):
95 Wanted for arrest/extradition	35 919
96 Unwanted alien	659 347
97 Adult missing person	23 679
97 Minor missing person	33 623
98 Localization	94 292
99.2 Check/observation	38 341
99.3 Check observation	606

Politiet i de ulike landene kan forespørre informasjon fra andre land om personer og gjenstander eller bruk av opplysninger med henblikk på spaning (Mathiesen, 2000). Man vil her kunne holde kontroll med personer som er uønsket inn i Schengenområdet av sikkerhetsmessige hensyn eller på bakgrunn av manglende adgangspapirer. Selv om det kun er bestemte myndigheter som har adgang til å søke i SIS så er disse mangfoldige. Politi, toll og grensekontroll skal ha adgang. Alle landene bidrar med å holde systemet oppdatert (Mathiesen, 2000).

Man skal arbeide etter *tilgjengelighetsprinsippet*; dersom en stat har behov for informasjon i sin etterforskning som en annen stat sitter på skal denne gjøres tilgjengelig for staten uansett (Kvam, 2008). Dette er et av de prinsippene som bidrar til å effektivisere systemet. Man gir også avkall på noe av den nasjonale suvereniteten ved at man kan søke i andre staters databaser uten tillatelse på forhånd (Kvam, 2008). I Schengenkonvensjonens artikkel 46 nr.1 (2007) understrekes det at en stat helt uoppfordret kan oversende opplysninger til en annen stat dersom man mener man er i besittelse av relevant informasjon som kan være til hjelp. Kritikk har vært rettet mot at systemet kan fremstå som noe tungrodd med en byråkratisk struktur, og det påpekes i rammebeslutningen av 18.desember 2006 at

informasjonsutvekslingen og etterretningen skjer for lite effektivt (Kvam, 2008). Dette vil kunne bidra til effektiviseringen.

Adgangen til SIS skal være kontrollert, men totalt sett har systemet mange adgangspunkter og brukere. I følge Schengenkonvensjonen skal grensekontroll, politi og også «national judicial authorities» ha adgang (Schengenkonvensjonen, 2007 art.101). Også personell som behandler visum-søknader og søknader om oppholdstillatelse, eksempelvis UDI skal ha tilgang. Det understrekes riktignok at de kun skal ha den tilgangen de trenger for å kunne utføre sitt arbeid, altså ikke tilgang til det totale systemet. Hvert land skal sende Eksekutivkomiteen en liste over de som har tilgang i deres stat og hva denne informasjonen brukes til (Schengenkonvensjonen, 2007 art.101). Dette legger opp til forskjeller landene i mellom.

Hovedvekten av ansvaret legges på den som legger opplysningene inn i SIS, denne skal påse at opplysningene er nøyaktige, oppdaterte og rettslig begrunnet (Schengenkonvensjonen, 2007 art.105).

2.2.2 Det nye SIS

Ingenting er statisk og SIS er intet unntak. Også dette systemet har gjennomgått en kraftig utvikling.

Det nye SIS, *SIS II*, har i flere år vært under planlegging, og veien har vært lang med flere brutte tidsfrister. Første planlagte lanseringstidspunkt var 2006, neste planlagte lanseringstidspunkt i rekken var 2013. Om det i det hele tatt kom til å skje på noen år var uvisst. Men så; en måned før punktum settes i avhandlingen skjer det: 9.april 2013 lanseres SIS II for alle medlemsland i Schengen (European Commission, 2013).

Det er flere årsaker til at man har ønsket å lansere en ny utgave av SIS; for det første gikk 10 nye land inn i EU i 2004 som gjorde at det tekniske kapasitetsbehovet økte (Parkin, 2011a). Det originale SIS-systemet hadde kun kapasitet for tilknytning av 18 land. Man har også et behov for å kunne registrere biometriske data som fingeravtrykk[2] og fotografier. Nye

[2] De nye registreringsalternativene og andre lovendringer ifm. SIS er bygget inn i SIS-loven ved *Lov om endringer i lov 16.juli 1999 nr.66 om Schengen informasjonssystem (SIS)* (2008). Deler av endringsloven trådte i kraft 9.4.2013 ved lanseringen av SIS II.

varslinger i systemet har man også ønsket å bygge ut. Alt dette bringer systemet fra et «hit/-no hit» system over i en ny dimensjon som åpner for spørsmål av etisk art i større utstrekning enn tidligere. Det blir også et langt mer komplekst system med hensyn til etterforskning (Parkin, 2011a). I presseskrivet nevnes det at SIS II legger vekt på muligheten for etterlysning av barn (European Commission, 2013). Dette vil ikke minst kreve skjerping av de etiske retningslinjer knyttet til SIS. SIS II gir også mulighet for *sammenkobling av varslinger*; eksempelvis en person og et kjøretøy, som ikke var mulig i første generasjon av SIS (European Commission, 2013). Dette vil øke muligheten for å kunne benytte SIS II mer effektivt i etterforskning. Muligheten for å legge inn varslinger om stjålne båter, luftfartøy og containere er også nytt med SIS II (European Commission, 2013). SIS II er med dette et system som inneholder et meget detaljert og komplekst datainnhold.

Kombinasjonen av at man startet arbeidet med systemet uten at man hadde klart for seg hvordan de tekniske funksjonene skulle være i kombinasjon med tidspress frem til de nye landenes medlemskap i 2006 har gjort til at man har fått store forsinkelser i arbeidet (Parkin, 2011a). Kostnadene for det nye systemet har også økt med 500 % fra det estimerte i 2001 (Parkin, 2001). I presseskrivet går det frem at SIS II har kostet € 167 784 606 (European Commission, 2013).

I mellomtiden har man måttet slå seg til ro med den midlertidige løsningen såkalt ”SISOne4All”. Man har på veien benyttet private aktører i utviklingen av systemet, noe som har ført til at man også har måttet ta hensyn til deres meninger og interesser. Det går imidlertid frem i presseskrivet at en privat aktør vi stå for driften av det sentrale systemet til SIS II (European Commission, 2013).

2.2.3 SIRENE

SIRENE (*Supplementary Information Request at the National Entries)* er et system for tilleggsinformasjon om personer og gjenstander for SIS mellom de ulike landene og fungerer som et teknisk støttesystem for bilateral og multilateral utveksling av informasjon (Mathiesen, 2000). Til forskjell fra SIS er det her snakk om ikke-standardiserte ”myke” opplysninger. SIS inneholder stort sett bare standardiserte opplysninger, mens gjennom SIRENE kan man få tilleggsopplysninger som supplerer informasjonen i SIS (Mathiesen, 2000). Informasjonen

kan eksempelvis være mer utfyllende opplysninger om personer eller dokumenter man anser som nødvendig. Med dette er *kommunikasjon* et viktig nøkkelord for denne virksomheten. Kommunikasjonen i SIRENE kan være både muntlig og skriftlig og man har mulighet for å sende bilder og fingeravtrykk til mottakeren – her benyttes systemets eget postsystem. SIRENE er langt mindre regulert enn SIS. SIRENE som system var opprinnelig ikke nevnt i Schengenkonvensjonen (Mathiesen, 2000).

2.3 Andre Schengenrelevante systemer

SIS og SIRENE står ikke alene som systemer for registrering og overvåking i EU selv om SIS representerer det største og mest omfattende systemet. På 90-tallet kom det til en rekke andre systemer og det ser ut til at utviklingen ikke er over. I tillegg til SIS er det flere systemer som har som formål å opprettholde kontroll med reisende til og gjennom Europa. Mathiesen (2000) beskriver det hele som et stjernedryss av systemer og skriver: «*Schengen befinner seg i dag så å si som den sentrale stjerne i dette stjernedrysset, som flere av de andre «stjernene» er relatert til og dras mot»* (Mathiesen, 2000 s.68).

Selv om det er SIS som er ledestjernen for avhandlingen er det likevel viktig å være klar over *det totale overvåkingsbildet* som SIS er en del av. De ulike systemene og organene inngår i et samarbeid, noen tettere enn andre, og det er nærliggende å tro at utviklingen går i retning av en mer integrert løsning. Jeg nevner de største forordningene.

2.3.1 Visa Information System (VIS)

VIS er et system som benyttes av Schengenlandene til å utveksle visum-informasjon og for å holde kontroll på visumsøkere (European Commission, 2012, ec.europa.eu 2.3.2013). Systemoppbyggingen minner noe om SIS da det består av et sentralt system som kommuniserer med de ulike medlemslandene (European Commission, 2012, ec.europa.eu 2.3.2013).

Informasjon om personers utfall på søknad om å få oppholde seg eller reise gjennom Schengenland vil kommuniseres via systemet (European Commission, 2012, ec.europa.eu 2.3.2013). Man vil fra tredjeland legge inn informasjon om visum-søkere som ønsker å entre Schengenområdet (statewatch.org 2013a 2.3.2013). Når personen reiser inn i et Schengenland vil man kunne sjekke fingeravtrykk, fotografi og persondata i systemet for å kunne identifisere en person (European Commission, 2012, ec.europa.eu 2.3.2013). På denne måten vil man raskt kunne avsjekke på en grensestasjon om en person er rettmessig eier av dokumentene som fremvises, og man vil kunne avdekke falske papirer eller stjålne dokumenter. Opplysninger vil lagres i VIS i 5 år og kan benyttes ved flere innreiser før de må fornyes. Nasjonale autoriteter og Europol kan be om tilgang til VIS, men det er hovedsakelig personell på grensestasjoner som skal benytte systemet (European Commission, 2012, ec.europa.eu 2.3.2013). Det er til dels likhet med SIS og VIS da det er lagt opp til en sentral database, med informasjonsstrøm fra databasen til medlemslandene (europa.eu, 2010 23.2.2013).

Det er altså ingen direkte kobling mellom SIS og VIS, men det er et system som vil kunne ha en supplerende funksjon.

2.3.2 Eurodac

Schengen-samarbeidet går som vist i hovedsak ut på å holde uønskede inntrengere ute fra medlemslandene med alt det dette innebærer. Schengenkonvensjonens asylkapittel ble 26.april 1994 erstattet av *Dublinkonvensjonen* (Mathiesen, 2000). Dette ble også godtatt av Norge. Dublinkonvensjonen fremmet det formålet at man skulle opprette et register for å registrere alle asylsøkeres fingeravtrykk i tillegg til andre persondata i en database; *Eurodac-registeret* (Mathiesen, 2000). Man kan på denne måten ved hjelp av fingeravtrykk undersøke om en asylsøker har krysset grensene på ulovlig grunnlag, og man kan også finne ut om asylsøkeren tidligere har søkt asyl i et annet medlemsland (http://europa.eu/ (2010) 23.2.2013). Registrering av fingeravtrykk var en av aksjonsplanene for Schengen for å bekjempe illegal immigrasjon, og man kan også utveksle fingeravtrykk gjennom SIRENE (Mathiesen, 2000). Dette vil muliggjøres i SIS II (Parkin, 2011a). I utgangspunktet er Eurodac og SIS uavhengig av hverandre, men det er særdeles viktig å være klar over sammenhengen

som Mathiesen (2000) uttrykker det; *«(…) som så mye annet i Schengensammenheng, er det de uformelle kontrakter og overenskomster som teller, samtidig som det i meget stor grad er de samme personer som lager planer og treffer beslutninger i og utenfor Schengen»* (Mathiesen, 2000 s.73). Det er på bakgrunn av dette nærliggende å anta at man går mot en integrert løsning.

2.3.3 Europol

Til sammenlikning med *Interpol* har EU's eget organ *Europol* (The European Police Office) mandat til å arbeide på tvers av landegrensene til medlemslandene, også med Norge, og samarbeider i tillegg med ikke-europeiske land (europol.europa.eu/ 2013 23.2.2013). Deres uttalte hovedmål er til forskjell fra Schengen å arbeide med etterforskning av alvorlig grenseoverskridende kriminalitet som terrorisme og alle former for organisert kriminalitet. Målet er å bistå alle medlemslandene i deres arbeid mot internasjonal kriminalitet og bistå til å skape et tryggere Europa (europol.europa.eu/ 2013 23.2.2013). Europol tar sikte på å bli en av de mest sentrale aktørene for informasjon i Europa, også ved å bygge videre på sitt system for informasjonsutveksling «Europols Secure Information Exchange Network Application» (SIENA) (europol.europa.eu/, 2013 23.2.2013). Man har også sett at det er behov for å gi Europol tilgang til Eurodac.

Europol har tilgang til SIS; *«(…) (Europol) shall within its mandate and at its own expense have the right to have access to, and to search directly, data entered into the Schengen Information System in accordance with Articles 95, 99 and 100»* (Schengenkonvensjonen, 2007 art.101A). Regelverket understreker at Europols bruk av informasjon i SIS må godkjennes at den medlemsstat det gjelder, og Europol kan heller ikke kommunisere dette videre dersom det ikke er godkjent av medlemsstaten (Schengenkonvensjonen, 2007 art 101A). Regler knyttet til forbud mot å laste ned eller knytte andre databaser opp mot SIS er også beskrevet. Det er også kun definerte ansatte i Europol som skal ha adgang til SIS (Schengenkonvensjonen, 2007 art.101A).

Alle land har et nasjonalt kontaktpunkt opp mot Europol. I likhet med SIS er kontakten med Europol i Norge lagt til Kripos.

2.3.4 Prümkonvensjonen

Prümkonvensjonen, som også går under tilnavnet Schengen III, er en avtale som går ut på å effektivisere utveksling av informasjon i EU (Jones, 2012).

Avtalen ble i første omgang signert av Belgia, Tyskland, Spania, Frankrike, Luxembourg, Nederland og Østerrike i 2005 (Prümkonvensjonen, 2005). Målet har vært å intensivere samarbeidet på grensene spesielt med tanke på å bekjempe transnasjonal kriminalitet og ulovlig innvandring. Avtalen har en del likhetstrekk med Schengenavtalen, men man ønsker med Prümsamarbeidet å løfte samarbeidet og arbeidet mot de nevnte aspekter et hakk videre. Dette vil inkludere å forbedre informasjonsutvekslingen og gjøre den mer *automatisert* og *effektiv*. Man skal kunne søke i andre nasjoners registre for DNA, fingeravtrykk, bilregistreringsdata og persondata. Det skal opprettes et nasjonalt kontaktpunkt i alle nasjoner (Prümkonvensjonen, 2005).

Foreløpig ligger man langt etter målsettingen om den effektive informasjonsutvekslingen, dette fordi det er store tekniske forskjeller mellom de ulike landene, samt at implementeringen krever midler (Jones, 2012). Norge har godtatt avtalen (Jones, 2012).

Det er nærliggende å anta at Prüm vil veves tett inn i SIS II da dette systemet vil ha rom for utveksling av fingeravtrykk og DNA i tillegg til ordinær persondata.

2.3.5 Passenger Name Record (PNR)

Ved booking av en flybillett må man oppgi en mengde personinformasjon som vil utgjøre dataene i Passenger Name Record (PNR) (Statewatch.org, 2013a 2.3.2013). Informasjonen som samles her består av over 30 ulike elementer (Boehm, 2009). I EU ser man nå på muligheten for å benytte informasjon hentet fra PNR for EU's grensevakter (Statewatch.org, 2013a 2.3.2013). Man vil da få tilgang til reisendes personinformasjon. På denne måten kan man få større kontroll på reisende og personer som ikke minst er i transit i påvente av å reise videre, da man ønsker å bekjempe eksempelvis faren for smugling. Det er noe uenighet om dette vil ha noen særlig effekt, men Europakommisjonen har allikevel satt av €50 millioner for å opprette PNR databaser i medlemslandene.

Man vil ved hjelp av i grunn nokså overfladiske data kunne lage en profil av reisende og vil på bakgrunn av dette vurdere som man skal foreta seg noe (Statewatch.org, 2013a 2.3.2013). Det kan være grunn til å anta at dette vil kunne dra med seg en viss stigmatiserende effekt. Man kan også analysere data mer automatisk der man vil se etter mønstre og kan ha mulighet for å dra paralleller mellom data, såkalt «data-mining» (Statewatch.org, 2013a 2.3.2013). Storbritannia ser nå på muligheten til å utvide denne overvåkingen over flytrafikk til også å gjelde båt- og togtrafikk (Mathiesen, 2013).

Totalt sett representerer overvåkingssystemene og de ulike foranstaltningene et enormt lappeteppe av kontroll. Og jeg har her langt på vei latt være å nevne alle. Som nevnt tidligere er det er også en feilantakelse at man har satt i gang disse systemene i kjølvannet av terroren man har sett de siste årene. TREVI, som var en annen nettverksgruppe for politisamarbeid i Europa ble startet allerede i 1976 med fokus på bekjempelse av terror og som koordinerende enhet for politiet (Bunyan, 1993). Sheptycki nevner at det var 7 «friends of TREVI», og Norge var en av disse (Sheptycki, 1995).

Nettverket av kontrollorganer består både av formelle og mer uformelle samarbeidsformer, ispedd en stor porsjon informasjonsteknologi som gjør terrenget uoversiktlig og komplisert (Sheptycki, 1995).

Selv om det er SIS som vil spille hovedrollen i avhandlingen, er det viktig at man er klar over hvordan de ulike kontrollsystemenes tentakler veves inn i hverandre og hvordan samarbeidet fungerer, selv om det ovenstående ikke er en utfyllende beskrivelse. I vurderingen av SIS må man på bakgrunn av dette ta i betraktning *det totale overvåkingsbildet* som SIS er en del av.

2.4 Risen bak Schengenspeilet

Teknologien har de senere årene gjort store fremskritt som har gjort det mulig å drive politiarbeid, overvåking og informasjonsutveksling på tvers av landegrensene enklere og i større skala enn tidligere. Det er uten tvil store fordeler med dette. Globaliseringen setter sitt preg også på kriminaliteten; den spres hurtigere over grensene og narkotikahandel og trafficking ser ut til å ekspandere. Det å kunne samarbeide med politikolleger i andre land for

å få bistand og informasjon i bekjempelsen av organisert kriminalitet vil kunne gagne alle i et samfunn.

Men medaljen har sin bakside. I kjølvannet av systemene har det blitt satt pekepinn på de ulike faremomentene som systemene, spesielt SIS representerer. Dette vil fungere som bakteppe for diskusjonen videre, og det vil senere bli sett på hvordan mine informanter vurderer dette i dag.

2.4.1 Utilsiktede virkninger

Lover og regler man setter i kraft, systemer man lager og samarbeid som settes i gang blir til med det formål for øyet å skape noe bedre. Men ofte vil det man forsøker å oppnå dra med seg konsekvenser man i utgangspunktet ikke har reflektert over, eller at man har valgt å ta en sjanse. I Schengen-samarbeidets tilfelle har man som vist vært klar over at man må kompensere med noe når man har valgt å legge ned de indre grensene. Thomas Mathiesen (2005) omtaler de «ikke-tilsiktede virkninger» som et forhold mellom «idealer» og «realiteter». *«Idealet tilsier at de uttalt tilsiktede virkninger skal oppnås, mens realitetene ofte er at slike virkninger ikke fremmes, eller bare fremmes i begrenset grad, og at tiltak har andre virkninger enn de som var planlagt og ventet»* (Mathiesen, 2005 s.98).

Her vil en del av disse utilsiktede virkningene presenteres, for så å pensles mer utførlig ut senere.

2.4.2 Datasikkerhet og personvern

Et av de største ankepunktene knyttet til SIS gjelder farer knyttet til datasikkerhet, rettssikkerhet og personvern. Beskyttelse av personopplysninger og datasikkerhet er viet et eget kapittel i Schengenkonvensjonen. Dette viser at man har dette temaet i bevisstheten, men det er allikevel en del spørsmål som har reist seg og som fremdeles er aktuelle.

Det kan være store nasjonale forskjeller i krav til *datasikkerhet*, *kvalitet* og *kontroll* med opplysningene mellom de ulike landene (Mathiesen, 2000). Det er også en mulighet til stede

for at det vil være forskjeller i *bruken* av opplysningene, og at regelverket kan gi rom for skjønn (Mathiesen, 2000). Dette kan ha stor innvirkning på individers personvern og rettssikkerhet.

Det er et faremoment at Norge og andre land legger inn opplysninger i SIS uten at man har kontroll på hvordan opplysningene vil anvendes når de blir hentet ut i den andre "enden". Når man legger inn info i systemet i et land kan det tas ut i et annet land under helt andre forutsetninger med en helt annen lovgivning (Mathiesen, 2000). Norge har sine bestemmelser, men opplysningene kan behandles helt ulikt etter et annet lands lovgivning i en annet stat. Behandlingen av opplysningene er i stor grad avhengig av den lokale rettskulturen. Vi vet at terskelen for å bli registrert i SIS også kan være svært variabel fra land til land; noen steder kan man bli lagt inn i systemet for minimale lovovertredelser eller at man bare er mistenkt (Brouwer, 2008). «*Sådanne rettskulturelle forskelle er en achielleshæl for en regulering af denne type*» (Blume i Mathiesen, 2000).

Når hvert lands lovgivning gir bestemmelser for hvordan SIS behandles kan dette skape en stor utfordring. Det er rettet kritikk mot at det ikke finnes en felles regulering (Mathiesen, 2000). Det er riktignok utarbeidet en håndbok for SIS, den såkalte «SIS-håndboken», men denne er ikke tilgjengelig for andre enn politiet og vil for en utenforstående være umulig å få fatt i. Man har også Schengenkonvensjonen som styrende element som beskriver reglene for bruk av SIS. Det står likevel ikke til hinder for ulik tolkning eller bruk/misbruk. Det kan nevnes at før Schengenkonvensjonen var politisamarbeidet i form av Interpol og Trevi ikke regulert ved skriftlig rettsgrunnlag (Kvam, 2008). Slik er Schengenreglene om politisamarbeid nyskapende i så måte (Kvam, 2008).

Et moment som kan tenkes å spille en rolle er at hvert enkelt land har det økonomiske ansvaret for implementeringen og driften av SIS nasjonalt (Schengenkonvensjonen, art.119). Ut fra den generelle økonomiske situasjon i Europa, og ikke minst de senere års kriser kan det være aktuelt å reise spørsmålet om dette kan ha sitt å si for SIS. Det kan kanskje være grunn til å anta at personvern og datasikkerhet i et IT-system ikke er høyest på prioriteringslisten når et land er i ferd med finansielt å gå dukken? Selv om Norge som vil bli vist senere tilsynelatende har nokså ordnede forhold er det grunn til å tro at dette kan være noe variabelt mellom landene.

Et annet moment er at man kan bli overvåket og registrert uten at man er klar over dette (Mathiesen, 2000). Som Mathiesen skriver utgjør systemene en ukontrollerbar maktfaktor i samfunnet (Mathiesen, 2000).

2.4.3 SIS II

Punktene av kritikk som rettes mot SIS øker i takt med at systemet i seg selv eser i omfang.

Prosessen med SIS II har vært lite gjennomsiktig og systemet har blitt til på en udemokratisk måte (Parkin, 2011). Den samme kritikken har også blitt rettet mot dagens system.

I stedet for å ha et overhengende rettsdokument har SIS II blitt til på bakgrunn av ad hoc justeringer av regler man finner i Schengenkonvensjonen fra 1990 (Parkin, 2011a). Det har også vært påpekt at siden systemet skal være så fleksibelt og med slike store proporsjoner har det vært vanskelig å forutse hvilken form systemet endelig vil ta (Parkin, 2011a). Det kan virke som at «veien har blitt til underveis som man har gått».

Man reiser også spørsmål om man med det nye systemet har forsøkt å komme noe videre med hullene i datasikkerheten fra SIS I (Parkin, 2011a). To kategorier av problemer har tydelig vist seg hittil med SIS 1: 1) Problemer med hensyn til datakvalitet som skyldes ulik praksis landene i mellom med å rapportere borgere i tredjeparts-land. 2) Man er hindret fra å endre/varsle feilaktige oppføringer, dette både på grunn av lovmessige og praktiske hinder (Parkin, 2011a).

Man har nå utformet strengere regler for dataoppbevaring, og også muligheter for å straffe ulovlig oppbevaring av data eller unøyaktige oppføringer (Parkin, 2011a). Det påpekes som kritikkverdig at regelverket ikke sier noe om at personer skal varsles når informasjon om en blir lagt inn (Parkin, 2011a). Dette punktet vil tas opp mer utførlig senere under punkt for *innsynsrett.* Problemer knyttet til at innsyn, samt endring og sletting av feilaktige opplysninger vil bero på lovgivning i det enkelte land kan føre til forskjellsbehandling. Men det har ikke blitt gjort noe for å bedre rettighetene til individet på dette punktet med de nye reglene (Parkin, 2011a).

Det er liten tvil om at SIS II kommer til å bli langt mer kompleks enn første generasjon av SIS. Mye av det som følger med SIS II som bruken av biometriske data, inter-linkage (sammenkobling) av varslinger og inter-operabilitet mellom EU-databaser reiser en del etiske spørsmål knyttet til individers rettigheter (Parkin, 2011a). Bruken av biometriske data i blant annet grensekontroll har blitt kritisert for sin mulighet for å medføre feilbarlighet og at den kan være utsatt for svindel. Man kan eksempelvis gjøre et søk bare ved bruk av fingeravtrykk i fremtiden. I følge Article 8 skal personlig data kun innsamles for spesifikke og legitime årsaker. Man er redd for at det vil bli samlet inn data om personer som er mistenkelige og ikke siktet i en sak – dette er kritisert for å være upassende i et demokratisk samfunn (Parkin, 2011a).

Det at man eksempelvis kan lagre data om kriminelle og deres familiemedlemmer kan føre til stigmatisering av kategorier av mennesker, for eksempel de som søker opphold og statsborgerskap i EU (Parkin, 2011a). Siden SIS brukes både med hensyn til kriminalitetsbekjempelse og for innpass til Schengenområdet kan en immigrant bli satt under lupen ved hjelp av overvåking som et kriminalitetsbekjempende tiltak. Man kan stå overfor en sterkere assosiasjon mellom immigrasjon og kriminalitet, noe som kan føre til at dette vil gå utover uskyldige personer. Man kan slik havne i en kategori av *potensielt risiko-beheftede* og dette kan stå i motsetning til EU's egne prinsipper om diskriminering (Parkin, 2011a).

2.4.4 Flyt av kriminelle?

Den friere menneskestrømmen gjennom Europa har gjort sitt til at vi har fått en slags «intern-globalisering» i større grad innenfor Schengens grenser. Norge er et rikt og mindre risikofylt land enn mange andre. Manglende utlevering samtidig som vi er i utakt med de omkringliggende landene kan føre til at Norge er i en sårbar og utsatt posisjon (Kvam, 2008). Det er en kjensgjerning at kriminelle ofte reiser til nærliggende land utenfor sitt eget for å planlegge fremtidige operasjoner, og dersom man har blitt beskyldt for å begå slike handlinger kan Norge være et av de mer gunstige landene å oppholde seg i. Noen vil frykte at Norge på denne måten kan bli en «base» for kriminelle (Kvam, 2008). Flyten av mennesker som søker seg til en bedre fremtid borte fra sitt hjemland ser også ut til å ha økt i kjølvannet av Schengen-samarbeidet. Noen vil fra et noe pessimistisk ståsted si at Norge ender opp som

en «fristat» for kriminelle etter hvert som muligens enda flere avtaler kommer til (Kvam, 2008).

Noe som er med på å komplisere det hele, spesielt for Norges del er at norske tollmyndigheter i skrivende stund ikke kan gjøre søk i SIS, *noe tollmyndighetene i andre land har mulighet til*. Dette er med på å sakke prosessen og gjøre den lite effektiv, samt at for Norges del vil kontrollen bli dårligere enn i andre land (Kvam, 2008). Dette vil kunne ha sitt å si for oppklaring og sjekk av stjålne biler og liknende som ofte er aktuelt på grensene.

Nedbyggingen av bevoktningen på grensene landene i mellom vil føre til at det blir lettere også for kriminelle å flytte på seg, og man forsøker å løse dette med kompenserende tiltak. Tiltakene består som vist i at man vil forsterke kontrollen på yttergrensene i Schengen, samtidig som man må legge opp til økt kriminalitetsbekjempende arbeid innad (Kvam, 2008). Mange vil reise spørsmålet om det er sannsynlig at terrorister og andre vil gjøre seg kjent med systemet og forsøke å opptre enda mer skjult enn i dag for å unngå å etterlate seg spor.

Kombinasjonen SIS som utvikler seg til et enda mer komplisert informasjonssystem og de samarbeidende og sidestilte systemer og organer gjør sitt til at vi står overfor et enormt overvåkingsmaskineri som bidrar til å gjøre Europa langt mer gjennomsiktig. Hva har egentlig bidratt til denne utviklingen?

3 Overvåking i samfunnet – forsøk på forklaringer

Samfunnet er gjennomsyret av overvåking. Alt fra dagliglivets rutiner til handlinger av mer alvorlig karakter kan etterlate seg digitale spor og vi samler og tar vare på denne informasjonen i stor utstrekning.

Hva kan forklare fremveksten av dagens overvåking? Er samfunnet blitt så farlig at vi er helt avhengig av dette arbeidet, eller kan man stille spørsmålet annerledes; overvåker vi i dag fordi det er mulig?

3.1 Et panoptisk samfunn?

Samfunnet er i ferd med å bli mer og mer gjennomsiktig – det er gjennomsyret av overvåking og kontroll (Foucault, 1975). Det er et bevoktningens samfunn.

I utgangspunktet treffer ingen dette mer midt i hjertet enn Michel Foucault (1975). Antakelig har heller ingen teoretiker fått så mye publisitet rundt teoriene sine knyttet til feltet. De fleste teoretikere vil likevel hevde at man ikke kan basere seg på hans teorier, men det fortjener en plass da det er fruktbart som et ”bilde” til inspirasjon. Jeg har valgt å inkludere Foucaults bidrag i min avhandling da det vil være å overse et av de mest sentrale og klassiske perspektivene rundt teoretiseringen av overvåking dersom dette utelates. Spørsmålet blir hvordan dette kan kobles til overvåkingen som drives i dag.

Jeremy Benthams ”Panopticon” må forstås som en maktmekanisme i form av en overvåkingsstruktur – opprinnelig en modell av et fengsel spesielt egnet for overvåking (Bentham i Foucault, 1975). *Panopticon* er et sammensatt gresk ord med betydningen ”se alt” (Foucault, 1975). I dette fengselet vil fangen alltid være synlig og klar over dette, og slik vil makten fungere automatisk. Modellen er designet slik at fengselsvokterne kan overvåke fangene hele tiden, men det er også innrettet slik at *fangene ikke er klar over når de blir overvåket* (Foucault, 1975). Foucault drar paralleller til dagens overvåkingssamfunn – overvåkingen kan være til stede uten at man er klar over at man iakttas og får slik sin automatiske effekt. Man har gått i retning av en mer usynlig form for overvåking. Man kan

selvsagt stille spørsmålet om dette fungerer i like stor grad i dag dersom folk flest ikke er klar over overvåkingssystemene som finnes.

Dagens overvåking kan passe godt inn i den panoptiske tankegang. Gjennomsiktigheten i fengselet ligger ikke nødvendigvis til grunn, men det at man aldri vet om man overvåkes kan være sammenfallende med dagens overvåking. Panopticon er en modell av et fengsel som er gjennomsyret av disiplinære mekanismer og Foucault påpeker at denne modellen har est ut i samfunnet (Foucault, 1977). Dagens overvåkings skjulte og subtile karakter ved at den i stor grad består av teknologiske elementer vil i større grad kunne føre til at man glemmer at den finnes eller ikke er bevisst på dette.

I kjølvannet av den panoptiske tankegang har tanker blitt utviklet om hvordan samfunnet har blitt med hensyn til overvåkingsstrukturene. I følge Foucault (1977) har man gått fra et skueplassens samfunn der man så på offentlige henrettelser på torget til et samfunn der *de få kan se de mange.*

Thomas Mathiesen supplerer panoptikken og mener vi kanskje er vitne til et samfunn der de mange kan se de få ved medias hjelp og lanserer derfor *synoptikken* (Mathiesen i Tollberg, 1997). Er man på denne måten tilbake til skueplassens samfunn? Kanskje kan man tenke seg en kombinasjon mellom de to posisjonene.

3.2 Risikosamfunnet – har samfunnet blitt farligere?

Samfunnet vårt er preget av overvåking og det har tilsynelatende blitt langt farligere. Hva har skjedd med samfunnet vårt?

Den tyske sosiologen Ulrich Beck (1986) gir et viktig bidrag til å beskrive samfunnet slik det fremkommer i den moderne tid. Globaliseringen akselererer, miljøgiftene strømmer på, skogene våre utarmes og terrorismen øker (Beck, 1986). Men har samfunnet vårt blitt farligere, eller er det vårt blikk som har blitt skarpere? For å stille spørsmålet noe annerledes; har samfunnet blitt farligere og gjort denne utviklingen nødvendig, eller overvåker vi i større grad på grunn av teknologien som muliggjør dette?

3.2.1 Fra industrisamfunn til risikosamfunn

I følge Ulrich Beck (1986) er man i det moderne samfunnet ikke lengre i den grad preget av klassemotsetninger som tidligere, men av *redsel*. Moderniseringen er årsaken til dette og moderniseringen fører med seg mange skadevirkninger (Beck, 1986).

Man er ikke lengre opptatt av forskjellene mellom individene (Beck, 1986). Om man bor i by eller land, ens nasjonale og etniske tilhørighet er ikke lengre det avgjørende. Klassesystemene sprenges og alle står i utgangspunktet på lik linje overfor risikoen, og man tenker først og fremst på hvordan man skal beskytte seg selv. Vi er ikke lengre et klassisk industrisamfunn, men et *risikosamfunn.* Risikoen vi står overfor i dag skiller seg fra tidligere (Beck, 1986).

I risikosamfunnet til forskjell fra tidligere kan ikke trusselen tilskrives noe eksternt – vi har selv skapt trusselen (Beck, 1986). Risikoens fordeling fører til sosiale trusselsituasjoner. Selv om vi alle står likt overfor risikoen har den en tendens til å hope seg opp i de nederste lag (Beck, 1986). Han nevner at risikoen også har en *bumerangeffekt* der den kan slå tilbake på de som har skapt den – dette kan også gjelde de høyt oppe i samfunnet. Risikoen kan forstås som trusler og man vet ikke når det vil inntreffe. Man er ikke lenger preget av fattigdom men av redsel. Dette er et resultat av det moderne samfunn. Hvordan skal jeg beskytte meg selv? Risikoen vi står overfor i dag skiller seg fra tidligere.

Klasseskillene vil allikevel bevares ved at man som rik/høyt utdannet til en viss grad kan kjøpe seg vekk fra risiko; rent vann, sikkerhet og liknende. Slik vil risikofaktorene i stor grad bli værende i bunnsjiktet (Beck, 1986). Vi har slik sosiale forskjeller innenfor *utsettelsesfaren* for risiko (Beck, 1986). Men mange av farene vi møter i det moderne samfunnet står vi på lik linje ovenfor. Terror vil være et eksempel på dette. På denne måten har klassemotsetningene noe redusert relevans.

3.2.2 Morgendagens risiko

Risikoen kan forstås som trusler i fremtiden – det har ikke ennå inntruffet og man vet ikke når faren vil inntreffe (Beck, 1986). Vi handler i dag i stor grad for å forhindre og minimere morgendagens risiko. Vi jobber i større grad for fremtiden, ikke kun nåtiden eller fortiden

som nok i større grad har kjennetegnet politiarbeid til nå. Risikosamfunnets mål er at alle skal skånes fra "giften" (Beck, 1986). Dette er i tråd med dagens overvåkingsarbeid.

Politiets overvåkingsarbeid er i ferd med å bli mindre *reaktivt* og mer *proaktivt* (Pearsall, 2010). I likhet med at eksempelvis en økonom kan predikere svingningene i et marked, tar politiet i økende grad i bruk teknikker for å predikere sannsynlig fremtidig atferd basert på mønstre og tidligere hendelser. Dette er en voksende trend i politiarbeidet (Pearsall, 2010). Denne måten å arbeide på er ikke en ny teknikk for politiet, men det er *bruken av data* som tar dette til ett nytt nivå. Ved å benytte data, gjerne fra flere kilder vil man kunne tolke, beregne og forhåpentligvis forhindre fremtidige hendelser. Flere av systemene som benyttes av politiet i Europa kan derfor settes i sammenheng med Becks tanker rundt risikosamfunnet.

3.2.3 Information Overload?

Som vist er det ikke få systemer og organer som alle kjemper for de samme målene i Europa. Og disse er nok ei heller de siste vi ser. Disse systemene samler og prosesserer uhåndgripelige mengder av informasjon. Man kan reise spørsmålet; vil man kunne klare å nyttegjøre seg all denne informasjonen man samler opp? Mister man oversikten? En politimann beskrev arbeidet med å tolke datamaterialet hans avdeling hadde ansvaret for å studere som «*å drikke fra en brannslange*» (Sheptycki, 2007).

Med dagens muligheter innen teknologi og overvåking blir «alle» en potensiell trussel, et spørsmål som reises i denne sammenheng er om man «gaper over for mye», og gjør at prediksjonene inneholder for mye feil og for mye informasjon totalt til at de har noen særlig verdi (Zedner 2007, 2009 i Mathiesen, 2013).

Alt dette gjøres for å prøve å forsikre oss mot de truslene og farene som en dag måtte komme. Georg Apenes karakteriserer dette som «*å konservere høystakker for det tilfelle at det skulle vise seg at det er en nål i en av dem*» (Tb.no 13.1.2010). Dette er tilfellet for SIS der man lagrer informasjon dersom man anser det sannsynlig at en kriminell handling vil inntreffe i fremtiden. Dette gjelder også på personnivå der man på bakgrunn av tidligere handlinger eller beregninger av sannsynlighet og risiko forsøker å preventere og identifisere trusselbilder og eventuelle fremtidige hendelser.

Vi kan ikke være sikre på om det er kommet flere trusler til, eller om det bare er vårt blikk som har blitt skarpere (Beck, 1986). Man må håndtere redselen og utryggheten i risikosamfunnet. Dette blir nødvendig både privat og politisk, for i risikosamfunnet truer unntakstilstanden med å bli normaltilstanden. På denne måten er Becks teori sammenfallende med dagens politiarbeid. Man arbeider for å forhindre morgendagens risiko.

3.3 Rettspluralisme

For å kunne følge opp regelverket i Schengen-samarbeidet, samt drive informasjonsflyten mellom landene har man som vist bygget opp et formidabelt politisamarbeid som samarbeider om overvåking av uønskede og mistenkte personer. Siden dette politisamarbeidet involverer mange land med eget lovverk reiser det seg spørsmål knyttet til hvordan et slikt samarbeid rettslig sett kan fungere.

Alle medlemslandene må i teorien behandle og forholde seg til systemet på lik måte, og når flere land er involvert i et samarbeid av denne karakter vil det også si at regelverk må gjøres gjeldene på kryss av landegrenser. Politiet har i alle medlemslandene i Schengenområdet ett felles regelverk å forholde seg til som skal gjøre dette samarbeidet mulig, selv om landenes egne lover vil spille inn. Vi er med dette vitne til globalisering av politiarbeid, som samtidig vil bety globalisering av lover og regler. Da dette er et internasjonalt samarbeid trer man inn i et eget landskap i rettssosiologien; *rettspluralisme*.

3.3.1 Hva er rettspluralisme?

Man kan skille mellom *rettsenhet* og *rettslig pluralisme* (Dalberg-Larsen, 1994). Rettslig pluralisme henviser til sameksistens og/eller overlapping av lov- og normsystemer til forskjell fra en rettsenhet der lov og normsystemer lever «alene». Dagens rettsforhold utgjør et mangfold som ikke nødvendigvis lar seg avgrense nasjonalt. Dalberg-Larsen (1994) understreker at den rettslige enhet man tidligere har holdt sterkt fast ved kanskje i større grad har vært preget av rettslig pluralisme enn man har tenkt eksempelvis i middelalderen, selv om man nok beveger seg i retning av pluralisme i større grad enn tidligere. Den rettslige

pluralismen med en internasjonal dimensjon er et av de viktigste aspektene ved moderne rett vi er vitne til i dag (Dalberg-Larsen, 1994). Og kanskje har vi bare sett begynnelsen. Globaliseringen generelt og ikke minst globaliseringen av økonomien spesielt har gjort sitt til at lover bryter ut over landegrensene og gjør seg gjeldende flere steder. Schengen-samarbeidet kan derfor sees i lys av at vi gjennomgår en økt globalisering; verden blir «mindre» og vi knytter tettere bånd til og samarbeider med parter geografisk sett langt borte fra oss selv. Vi integreres i denne pågående prosessen på mange hold, også i justissammenheng.

Samarbeidet verden rundt er et nettverk bestående både av offentlige og i større og større grad private aktører. Generelt i EU vil man finne lover og regler som brer seg over mesteparten av Europa – disse kan komme i konflikt med de ulike lands nasjonale lover (Eskeland, 1988). Vi går her fra rettsenhet til rettslig pluralisme ved at disse legges til de ulike nasjoners egne lover. Noen ganger vil EU-lovene også gå fremfor de nasjonalrettslige (Dalberg-Larsen, 1994). Et land som Norge vil også kunne «tvinges» til å endre sine lover og regler under påvirkning fra internasjonalt hold. Vi står altså ovenfor en situasjon preget av rettslig pluralisme fremfor en rettsenhet.

Spørsmålet er om lovene som begynner å fungere flere steder mister rot og kommer ut av synet for kontroll. Begynner lovene nesten å leve på egen hånd? Lovene spres over landegrensene via ”usynlige” nettverk (Mathiesen i Deflem, 2008). Ofte er dette profesjonelle nettverk bestående av eksempelvis advokater eller økonomer som jobber og samarbeider internasjonalt og som bidrar til utviklingen i høyt tempo. Ulike lands aktører inngår avtaler som lenkes inn i hverandre horisontalt og som ligger vertikalt langt vekke fra sine lands egne systemer. På denne måten er de isolert fra kontrollinstansene i de ulike landene. Ofte vil disse lovene bli tatt inn som et tillegg til et lands egne lover, men vil etter hvert tas opp, bli ansett som valid og blir plassert sammen med landets gjeldende lover. På denne måten blir de godtatt (Mathiesen i Deflem, 2008). Det kan nok også være vanskelig å holde kontroll med dette siden denne utviklingen vil styres av «ekspertene» selv.

Det er blitt nokså vanlig at forskjellige sektorer i samfunnet lager egne lover (Mertens i Teubner, 1997). *Lex Mercatoria* er kanskje det beste eksempelet vi har på en «landløs» lov. Loven behandler internasjonale transaksjoner, og fungerer på et overnasjonalt nivå. Systemet blir ikke lengre forankret i et spesielt land, men er et transnasjonalt system og begynner på en måte å leve for seg selv (Mertens i Teubner, 1997). Thomas Mathiesen drar parallellen til den globale kontrollen på tvers av landegrensene med sin *Lex Vigilatoria* (Mathiesen i Deflem,

2008). Slik som Lex Mercatoria ligger på et overnasjonalt nivå uten nasjonal forankring viser Mathiesen med Lex Vigilatoria fremveksten av politisk og sosial kontroll på samme måte.

Det vil nok ikke være helt riktig å si at man ikke har noen form for nasjonal forankring, for ett sted må lovene ha sitt utspring og en link til en nasjonal lov. Dette er også kritikken av Lex Mercatoria begrunnet i. I følge Teubner kan globale lover mangle politisk og institusjonell støtte, men kan settes i sammenheng med sosioøkonomiske prosesser (Teubner i Teubner, 1997). Slik politiet kan operere i dag kan det kanskje være en ide å snakke om en slags *mobil rett* der man bringer med seg lover fra sitt hjemland inn i et annet?

Politisamarbeidet i Schengen kan knyttes opp mot dette. Dette er et samarbeid som i liten grad ser dagens lys og som de færreste er klar over. Politisamabeidet i Schengen og alle detaljene knyttet til dette har blitt besluttet av et så å si «usynlig» nettverk bestående av et fåtall, *en elite*, og på nasjonalt nivå og i befolkningen generelt har man vært lite innblandet i prosessen (Loader, 2002). Dette fåtallet av personer har bestemt alt fra hvilken retning utviklingen skal ta, innholdet og hvilket tempo utviklingen skal foregå i (Loader, 2002). I tillegg vil det være systemene som knytter landene sammen og svekker båndene mellom politiet ved de fysiske avdelingene (Mathiesen, 2013). Ved at systemene i større og større grad går inn i hverandre og blir liggende «over» landene får man i Schengenområdet et forsterket horisontalt samarbeid, men vertikalt «kobles» de ulike landene av, og systemene tar over (Mathiesen, 2013).

3.3.2 Rettspluralisme – endring i rettskultur

Vi ser også eksempler på at vår egen rettskultur endres og det er naturlig å se dette i lys av rettslig pluralisme. I Norge har vi hatt en god balanse mellom menneskers frie livsrom og samfunnsvernet, altså behovet for å beskytte borgernes interesse mot skade (Lund i Egeland, 2010). De senere årene tenderer dette til å gå i retning av at *samfunnsvernet veier tyngre enn vernet av individene* (Lund i Egeland, 2010).

Lund understreker at Norge har hatt et mildt inngrepsnivå, som nå er i ferd med å endre seg – man kan se på dette som en forflytning fra en liberalstat over mot en politistat (Lund i Egeland, 2010). Sanksjonene blir tyngre, og utviklingen av kontroll og overvåking ekspanderer, også i det private rom. Til slutt vil alle ende under lupen – «*hele befolkningen*

står som mistenkt under regimets paranoide blikk» (Lund i Egeland, 2010). Aktuelle eksempler er Schengen Informasjonssystem og Datalagringsdirektivet.

Vi importerer verdier og normer fra andre rettskulturer, dette fører til endringer i vår egen rettskultur (Lund i Egeland, 2010). Dette kan også settes i sammenheng med globalisering. Internasjonal rett får stadig mer betydning etter hvert som det gjør sitt inntog og dette vil skape et stadig mer konfliktfylt og uoversiktlig rettslig landskap (Mathiesen, 2005). Dette kan ha mye å si for enkeltindividers rettssikkerhet.

I følge Bowling og Sheptycki (2012) er utfordringene og spørsmålene som reiser seg i dette terrenget ikke få. Når lover og regelverk legges oppå hverandre får man en konflikt og det må avgjøres *hva* som til syvende og sist skal være gjeldende og *hvor* lovene skal gjelde. Det kan også reises spørsmål om *hvem*, eller om det er noen i det hele tatt som holder kontroll på det som foregår på kryss av landegrensene (Bowling og Sheptycki, 2012). Og det burde kanskje også være noen som kontrollerer kontrollørene?

3.3.3 Rettspluralisme og politisamarbeid i praksis

Dagens politiarbeid har vokst seg utover landegrensene, og rettspluralismen kan bidra til å forklare hvordan lovsystemer spres og benyttes internasjonalt.

Vi har i dag ikke et verdensomspennende politi per se, men vi har et transnasjonalt samarbeid (Bowling og Sheptycki, 2012). *Interpol* er det første og største skrittet til et verdensomspennende politi, men organisasjonen har ingen operative styrker. Det er fokuset på organisert kriminalitet og terrorisme som har gjort at dette politiarbeidet har ekspandert over landegrensene. Det er en vanlig tanke at kriminalitet i større og større grad spres globalt som igjen vil kreve et globalt politiarbeid (Bowling, 2009). Men med dagens teknologiske muligheter ser det ut til at politiet selv er en stor pådriver til globaliseringen av sitt arbeid (Bowling, 2009). Ofte vil betegnelsene «nettverk», «organisert» eller «global» kriminalitet gi et misvisende inntrykk av de faktiske forhold, spesielt slik det fremstilles i media.

Det *transnasjonale* politiarbeidet kjennetegnes ved at politiarbeid kan fortsette over en landegrense og inn i et nytt land – man trenger altså ikke stoppe på grensen (Bowling og Sheptycki, 2012). Til forskjell vil et *internasjonalt* politiarbeid henvise til samarbeid mellom

nasjoner uten at man krysser grenser. Flere steder i verden har politiet i nærliggende land inngått samarbeid. Benelux-området (Belgia, Nederland og Luxembourg) er et av disse, men også de Karibiske øyer. Disse områdene er godt egnet for et slikt samarbeid med tanke på de små avstandene. I Benelux-landene fikk man problemer med at kriminelle kunne skape store utfordringer for politiet da enkelte rømte rett over grensen til nabolandet. Dette resulterte i et politisamarbeid (Bowling og Sheptycki, 2012). I Europa vil Schengen-samarbeidet falle innenfor sistnevnte kategori. Et slikt samarbeid kan bidra til å øke effektiviteten til politiet ved å ha større spillerom, og man kan lettere flytte rundt på ekspertise som kan bistå etterforskning ved behov. Men samarbeidet har også sin bakside.

På verdensbasis har det blitt satt pekepinn på en del utfordringer knyttet til ekspanderingen av politiarbeid. For det første er det et problem at de gruppene som arbeider internasjonalt ofte er satt opp *ad hoc* med tanke på bekjempelse av terrorisme og organisert kriminalitet (Bowling og Sheptycki, 2012). Bekymringen er at disse konsentrerer seg kun om et lite område, men allikevel vil ta hånd om hele strukturen i det globale politiarbeidet (Bowling og Sheptycki, 2012).

Det at verden har blitt «mindre» også rettslig sett har gjort at man har vært vitne til en økende tendens til at land kan «shoppe» internasjonalt i ønskede lover og regler som passer til ens formål (Bowling og Sheptycki, 2012). Et eksempel her er belgiske myndigheter som ikke tillater avlytting, men som fikk svenske kolleger til å utføre dette for dem (Bowling og Sheptycki, 2012). Man kan selvsagt sette spørsmålstegn ved om det er en legitim fremgangsmåte fra politiets siden der man tar omveier rundt eget lovverk, og det er intet mindre ironisk.

Et annet fenomen som tiltar er at det over hele verden sitter personer i varetekt utenfor sitt eget land som følge av transnasjonalt politiarbeid (Bowling og Sheptycki, 2012). Disse kjennetegnes ofte av lav økonomisk status og mørk hudfarge (Bowling og Sheptycki, 2012). Spørsmål knyttet til stigmatisering kan også her reises. De som har falt ned i denne rettspluralistiske kløften vil gjerne ha dårligere rettssikkerhet og liten mulighet for å orientere seg i det rettslige terrenget. Man har også en brukerside i et slikt justismaskineri, og når det kan være en mulighet for at flere lover lever side om side kan dette gjøre brukerrollen vanskelig. Hvem skal ha ansvaret for å etterforske dersom en internasjonal operasjon skulle gå galt? (Bowling, 2009). Som Bowling (2009) påpeker er det flere sider ved «vanlige» former for politiarbeid som kan være en fare; det er lite gjennomsiktig og vi er tvunget til å

stole på ekspertisen. Spørsmål om korrupsjon, diskriminering og inkompetanse reiser seg knyttet til politiarbeid, og det er som Bowling påpeker lite trolig at transnasjonalt politiarbeid er «immun» mot denne problematikken (Bowling, 2009). Det er grunn til å tro at problemene har potensial til å kunne øke i takt med politiarbeidets ekspansjon.

I Schengen og i bruken av SIS vil man kunne komme i situasjoner der man rent praktisk kan oppleve at landenes nasjonale lover er så forskjellige at det vil ha innvirkning på arbeidet. I Schengenkonvensjonen art.94 står rutinen for hvordan man skal håndtere dette eksplisitt beskrevet:

> *«Where a Contracting Party considers that an alert in accordance with Articles 95, 97 or 99 is incompatible with its national law, its international obligations or essential national interests, it may subsequently add to the alert contained in the data file of the national section of the Schengen Information System a flag to the effect that the action to be taken on the basis of the alert will not be taken in its territory»* (Schengenkonvensjonen, 2007 art.94).

Dersom man legger inn en varsling til en annen medlemsstat må man også forsikre seg om at en arrestasjon er mulig under de gjeldene lover til den medlemsstaten der man legger varslingen, og ved tvil må man kontakte den andre staten og få dette avklart (Schengenkonvensjonen, 2007 art.95). Man skal alltid handle ut i fra ens nasjonale lover, og slik vil det kunne være store forskjeller i praksis innad i Schengenlandene. Som vil bli vist senere vil kontrollen med SIS også føres på bakgrunn av Schengenkonvensjonen og landenes egne lover.

Den rettslige diskursen vil ikke bare omfavne de som har begått en kriminell handling, men også de som kan være potensielt farlige (Bowling og Sheptycki, 2012). Dette er i tråd med Ulrick Becks (1986) bidrag og kan ses i lys av arbeidet som driver overvåkingen i dag.

4 Metodekapittel

Mitt prosjekt består i å finne ut i hvilken grad personvernet og rettssikkerheten til enkeltindivider er ivaretatt i Schengen-samarbeidet; spesielt med tanke på lagring av informasjon i Schengen Informasjonssystem (SIS), samt se på hvilke effekter Schengen-samarbeidet har hatt. Jeg har også ønsket å se nærmere på kritikerne og kontrollørene til systemet for kunne belyse mine spørsmål samt identifisere hvem disse egentlig er.

For å kunne forstå hvordan systemet fungerer både fra innsiden og hvordan det betraktes fra utsiden har jeg gjennom samtaler med sentrale personer knyttet til feltet skapt meg et bilde av hvordan systemet står i dag og hvilke utfordringer vi står overfor.

Valg av tema og spesielt problemstilling kan nok gi inntrykk av at jeg allerede har tatt standpunkt før prosjektet ble satt i gang. Et gjennomgående trekk ved litteraturen knyttet til Schengen-samarbeidet kretser rundt utfordringene og er for det meste kritisk innstilt. Et av hovedmålene med avhandlingen er å se nærmere på dette, også fra innsiden av systemet ved dets egne brukere. Siden jeg ønsker å stille ”utsiden” opp mot ”innsiden” har jeg hele tiden vært klar over at jeg kan avdekke synspunkter som for meg hittil var ukjente, og jeg har således vært forsiktig med å ta standpunkt på forhånd.

4.1 Utvalgsstrategi

For å kunne belyse problemstillingen i avhandlingen på en best mulig måte har jeg valgt å foreta dybdeintervjuer og dokumentstudier da dette har vært mest hensiktsmessig i forhold til problemstillingen.

Målet har vært å intervjue representanter som har ulik innfallsvinkel til tematikken og som representerer ulike sider slik at jeg kan få et mest mulig helhetlig bilde. Måten jeg har gjort min utvelgelse av informanter på kan betegnes ved begrepene *purposeful sampling*, eller *strategisk utvelgelse* (Johannessen, Tufte og Christoffersen, 2010). Det har vært viktig å få belyst spørsmålene ved å se på hvordan ulike aktører i nøkkelposisjoner på feltet oppfatter kontrollsamarbeidet og følgene for rettssikkerheten. Det er ikke nødvendigvis antallet som er avgjørende, men *hensiktsmessigheten* av informantenes deltakelse som er viktig

(Johannessen, Tufte og Christoffersen, 2010). Jeg mener at ved å velge ut representanter med ulik bakgrunn og ståsted i forhold til temaet, vil en på en måte kunne oppnå en viss form for representativitet av fagfelt ved personer som har en tilknytning til området. Jeg har derfor ønsket å snakke med personer som både er representanter for systemet, men også de som representerer motkreftene og kritikerne. Sett i forhold til sakens natur har jeg gjort utvalget på bakgrunn av å finne frem til de som best har forutsetninger for å uttale seg og/eller mene noe i saken. Utvalget har blitt foretatt i samråd med veileder.

I noen tilfeller har jeg mottatt tips fra mine informanter om personer og organisasjoner jeg bør kontakte og som kan ha noe viktig å bidra med. I enkelte tilfeller har jeg også mottatt verdifull kontaktinformasjon. Jeg har på denne måten benyttet meg av *snøballmetoden* (Johannessen, Tufte og Christoffersen, 2010). En del av mine informanter har også vært behjelpelige med å stille dokumenter og brev til rådighet som jeg nok ikke ville kommet over på egen hånd. Dette har vært svært nyttig i arbeidet.

Jeg vil i dette henseende understreke at temaet jeg tar for meg, spesielt politisamarbeidet, er et tema som er skjult og strengt taushetsbelagt. Det vil i intervjusammenheng si at selv om en informant eksempelvis på bakgrunn av sin juridiske kompetanse kjenner til overflaten av systemet og har meninger om hva utfordringene består i, er det et fåtall av mine informanter som har sittet med detaljkunnskaper om SIS. Og slik skal det også være. SIS er et system som benyttes av politiet, og det er politiet og deres nære kontrollører som skal kjenne detaljene i dette. På denne måten går det et skarpt skille mellom de som sitter som anvender eller kontrollør av systemet og de som betrakter det utenfra. Jeg håper jeg vil få vist dette, samt at ens ståsted kan ha sitt å si for ens fortolkning.

I tillegg til intervjuene har jeg benyttet dokumenter for å gå i dybden på aktuelle regelverk knyttet til Schengen. Dette har hovedsakelig bestått av konvensjoner og informasjon sentralt fra EU. Jeg har også benyttet kriminalstatistikk for å se på kriminalitetsutviklingen over tid. Dette er ingen utfyllende analyse, men et supplement.

4.2 Informasjon og anonymitet

Alle mine informanter har blitt informert skriftlig i forkant av prosjektet, og det har også i tilfeller vært en del korrespondanse i forkant av intervjuene per mail og/eller telefon. Jeg har grundig presentert mitt prosjekt og gitt informasjon om hva dataene fra intervjuene skal brukes til. Hovedformålet med dette har vært å gjøre all informasjon som er nødvendig tilgjengelig for informantene. På denne måten har jeg fulgt de forskningsetiske retningslinjene og oppnådd *informert samtykke* (Johannessen, Tufte og Christoffersen, 2010). Jeg vil jevnt over si at jeg har blitt møtt med en stor velvillighet til å stille til intervju, og de gangene der en intervjuavtale eller kontakt har vært vrien å oppnå, er det som regel tid det har stått på. Det har vært en relativt tidkrevende prosess å få avtalt intervju med mine informanter, da de alle har vært spredt i ulike organisasjoner og de er svært opptatt i sitt daglige virke. Likevel har jeg oppnådd intervju med alle jeg ønsket å oppnå kontakt med.

Ingen av mine informanter kan karakteriseres som representanter for en sårbar gruppe eller enkeltindivid, snarere tvert i mot. Det har kun vært et ønske fra tre av mine informanter om anonymitet på individnivå. Jeg vil ettertrykkelig understreke at de informantene jeg nevner ved navn har gitt sitt samtykke til dette. I de tilfeller der informantene ønsker å forbli anonyme vil jeg kun henvise til navnet på organisasjonen.

Jeg mener ellers at temaet er holdt på et makro-nivå og er av en slik art at sjansen for at noe som berøres vil kunne skade eller krenke enkeltindivider er liten. Men jeg har holdt de etiske sidene av forskning generelt in mente når jeg har utført feltarbeidet og databehandlingen i ettertid.

4.3 Mine informanter

Her vil jeg gi en fremstilling av mine informanter for å begrunne hvorfor disse ble utvalgt, samt kort fremstille settingen intervjuene ble foretatt i. Totalt er 9 personer intervjuet, 2 av intervjuene ble foretatt med to informanter samtidig etter deres ønske.

Kripos - Et av hovedmålene jeg har hatt i mitt arbeid har vært å oppnå kontakt med Kripos ved SIRENE-kontoret. Kripos representerer i Norge *innsiden* og *utøveren* av systemet, og det har derfor vært viktig for avhandlingen å få deres synspunkter lagt frem.

Det var en tidkrevende og komplisert prosess å oppnå kontakt og etter hvert en avtale med Kripos. Jeg kontaktet Kripos i en periode der deres tid var presset, men velviljen var heldigvis til stede. Skriftlig søknad måtte sendes til SIRENE-kontoret. De stilte en del krav til meg som besøkende og intervjuer hos dem, som gjør at jeg er tvunget til å beskrive dette noe nærmere. For det første har to av mine informantgrupper lagt inn krav til å se spørsmålene i forkant for så å godkjenne disse. Dette gjelder Kripos og EDPS (European Data Protection Supervisor). I Kripos' henseende måtte jeg sende over spørsmålene for gjennomlesing og godkjenning. Jeg mener jeg her i større grad var satt under lupen og frykten for å bli avvist gjorde at jeg måtte formulere mine spørsmål rundere og ikke så direkte som kanskje ønskelig var. Et par av mine spørsmål ble forkastet før intervjuet, da Kripos mente de ikke kunne svare på disse.

Kripos stilte med to informanter som jeg skulle intervjue i et og samme møte. Disse representerte ledelsen ved SIRENE-kontoret. Jeg fikk ikke tillatelse til å benytte opptaker under intervjuet. Dette førte til at jeg måtte basere meg på min hukommelse og notater fra intervjuet. Om dette er formålstjenlig kan selvsagt diskuteres. Det har også vært et krav fra Kripos' side at materialet skulle gjennomleses på forhånd før det gikk i trykken. Dette resulterte i et nytt møte. Mye hadde skjedd i løpet av året siden første møte med Kripos, og møtet viste seg å være svært nyttig. Jeg imøtekom alle krav fra Kripos da det var eneste løsning for å kunne få mulighet til å snakke med dem. I møtene med Kripos ble det allikevel åpnet for å stille oppfølgingsspørsmål og presiseringer ble gjort i en god samtale fra begge parter. På denne måten ble gjennomlesningen av spørsmålene på forhånd mer eller mindre en formalitet som muligens hadde lite for seg. Men det er nærliggende å tro at Kripos ønsket å sjekke hva jeg var «ute etter».

Jeg har et inntrykk av at mine informanter fra Kripos holdt litt igjen, og til tider kanskje ikke uttalte seg så grundig og utdypende fordi de rett og slett ikke kan si alt. Dette er forståelig ut i fra deres virksomhetsområde. Men jeg har ikke inntrykk av at intervjusettingen eller omstendighetene i for- og etterkant hadde noe å si for resultatene. Selv om alt var lagt til rette for en maktmessig skjevhet med to representanter fra Kripos i møte med meg som student sitter jeg igjen med et inntrykk av at selve intervjuet fortonet seg mer som en samtale, og det var en positiv opplevelse.

Det skal nevnes at jeg ønsket å snakke med en tidligere student ved Institutt for Kriminologi og Rettssosiologi som avla sin masteravhandling i rettssosiologi med svært lik tematikk som meg selv i år 2007. Han er nå ansatt ved SIRENE-kontoret. Mitt ønske var å sammenlikne

hans syn på mine spørsmål med minst en annen på kontoret med ulik bakgrunn også etter støtte fra veileder Thomas Mathiesen. Jeg ønsket å se om hans faglige bagasje kunne ha noe å si for hans syn på saken. Dette ønsket ble avslått fra Kripos' side, selv om han selv hadde et ønske om å stille.

European Data Protection Supervisor (EDPS) – EDPS er en autoritet som arbeider for å sikre personvern og god praksis innenfor de ulike EU-organene (edps.europa.eu, 2013a 5.2.2013). EDPS fungerer også som rådgiver og vil ha en rolle i klagesaksbehandling, og inspiserer og samarbeider med nasjonale datatilsynsmyndigheter (edps.europa.eu, 2013a 5.2.2013).

Representanten for EDPS jeg fikk snakke med er utdannet jurist og arbeider i avdelingen «Politician Consultation Unit». Intervjuet med representanten for EDPS foregikk per telefon av praktiske årsaker, da dette organet er situert i Brussel. Intervjuet ble foretatt på engelsk. Overfor EDPS kan det ha vært språket som i stor grad har ført til at det var ønskelig å se spørsmålene på forhånd. Jeg merket meg også i intervjuet at det nok var blitt tatt notater på forhånd for å kunne svare på spørsmålene best mulig. Dette fører meg over på tanker som at intervjuobjektet kanskje ikke satt inne med disse opplysningene og kunnskapene i detalj til vanlig, men hadde søkt opp dette i organisasjonen i forkant av intervjuet. Dette er og blir en antakelse. Uansett har jeg valgt å se på min representants svar på spørsmålene som de ”offisielle” svarene på vegne av EDPS. På den annen siden kan forberedelsen også ha ført til at jeg har fått mer utfyllende og gode svar og forklaringer enn jeg ellers ville ha gjort, samt at informanten hadde mulighet til å forberede seg til intervjuet på engelsk, da informanten har fransk som morsmål. På denne måten mener jeg at det at informanten fikk mulighet til å forberede seg til syvende og sist var formålstjenlig for intervjuet.

Georg Apenes – jurist og tidligere direktør for Datatilsynet og svært engasjert i debatten rundt personvern blant annet knyttet til Datalagringsdirektivet. I dag pensjonert og leder for foreningen *Digitalt Personvern*. Intervjuet ble foretatt per telefon med opptak på grunn av tidspress. Apenes var direktør i Datatilsynet når Norge gikk inn i Schengen-samarbeidet, dette var årsaken til at jeg anså Apenes som en verdifull informant.

Ketil Lund - tidligere Høyesterettsdommer og leder av Lund-kommisjonen. Intervjuet ble foretatt på hans kontor der han praktiserer som advokat ved advokatselskapet Lund & Co. Han er medlem av ICJ (International Commission of Jurists). Opptak ble benyttet under intervjuet.

Jon Wessel-Aas – Advokat og leder av International Commission of Jurists (ICJ) norsk avdeling. Meget engasjert i debatten rundt personvern og er med på å kritisere og holde liv i debatten. Intervjuet ble foretatt på hans kontor hos advokatselskapet Bing Hodneland. Opptaker ble benyttet.

Datatilsynet – min informant er ansatt på Tilsyns- og Sikkerhetsavdelingen og i ledelsen hos Datatilsynet. Tilsynsavdelingen fører kontroll med blant annet SIS hos Kripos. Min informants utdanningsbakgrunn og arbeidsområde skiller seg klart fra mine andre informanter med en Mastergrad i IT-sikkerhet og en Mastergrad i Business. Dette førte til at jeg fikk dekket inn mitt behov for konkrete og tekniske betraktninger rundt SIS. Intervjuet ble foretatt på hans kontor hos Datatilsynet. Opptaker ble benyttet.

Statewatch – Det har vært viktig for meg og min avhandling å oppnå kontakt med organisasjonen Statewatch i London. Statewatch er en av de største organisasjonene som «overvåker» det meste EU foretar seg og produserer et tidsskrift og en rekke artikler. Jeg møtte organisasjonens leder Tony Bunyan og en av hans ansatte, Chris Jones, i London.

4.3.1 Utvalgets sammensetning

Det er relativt stor likhet i utdanningsbakgrunn blant mine informanter. Dette vil heller ikke være unaturlig da temaet også omhandler de rettslige sidene ved SIS og Schengen i sin helhet. Disse har allikevel ulik erfaringsbakgrunn, noe som har gjort intervjuene verdifulle.

Spørsmålene som har blitt stillet til de ulike informantene har i stor grad vært avhengig av deres bakgrunn. Men jeg har så langt det har vært mulig forsøkt å stille de «universelle» spørsmålene til alle, dette for å få innblikk i likheter og ulikheter i synspunkter på spørsmål fra ulikt hold. Jeg har anstrengt meg for å forsøke å stille spørsmålene til mine informanter på en slik måte at de ikke har vært ledende og lagt føringer i unødig stor grad.

Det kan nevnes at det ville vært meget interessant å gjennomføre et kvantitativt studie der man ved et representativt befolkningsutvalg målte befolkningens kjennskap og holdninger til Schengen-avtalen. Dette ville koste langt mer tid og penger enn jeg har hatt til rådighet, men interessen er til stede. For å studere feltet faller valget som vist på studiet av dokumenter og kvalitativt feltarbeid.

5 Kontroll av kontrollørene

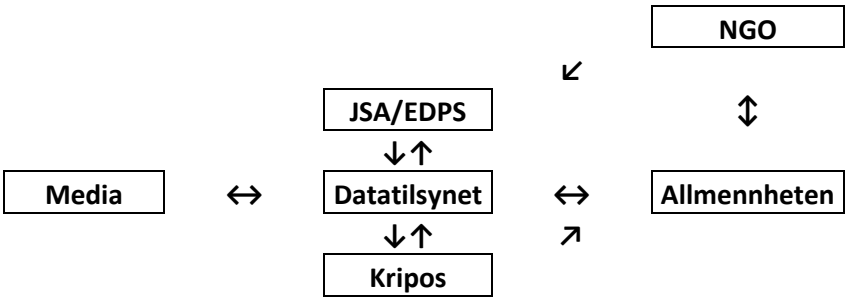
Ved å studere hvordan Schengensystemet fungerer og hvordan kontrollen føres, har det hele fått et «høk over høk» tilsnitt. For Norges del er Kripos den instansen som styrer systemene i deres daglige virke, men det er ikke slik at dette er unndratt kontroll fra andre instanser. Ikke bare vil en statlig instans som Datatilsynet fungere som kontrollør i et slikt system, men også private organisasjoner og privatpersoner vil spille en viktig rolle. Alle disse instansene vil fungere som kritiske røster og bidra til å ivareta de sivile rettighetene i det som kan virke som et uhåndterlig stort maskineri. Jeg vil her gi en gjennomgang av de organisasjonene jeg har sett nærmere på og forsøke å risse ut viktigheten av deres arbeid på dette området, samt det som påpekes av disse med hensyn til SIS. Gjennomgangen vil også basere seg på intervjuer. Hvem holder kontroll med hvem? Er Non-Governmental Organizations (NGO's) viktige for å ivareta rettssikkerheten? Er det noe nytte i deres arbeid?

Mine informanters synspunkter vil her bli løftet frem. Jeg har valgt å beholde skillet på aktør slik at det vil komme frem hvordan ens virksomhetsområde kan gjøre at en ser samme system med ulike «verdensbriller».

5.1 Kontroll- og informasjonsflyt

Ved en enkel modell ønsker jeg innledningsvis å vise hvordan det ser ut til at kontrollen og informasjonsutvekslingen fungerer knyttet til Schengen-samarbeidet og SIS. Modellen er ingen fasit, men bidrar med å sette et bilde på hovedtendensen.

Figur 1:



NGO's er plassert noe perifert da disse er uavhengige organisasjoner som i de fleste tilfeller ikke vil være bundet opp av forpliktelser overfor det offentlige. Som jeg vil vise senere kan dette være noe komplekst. Disse drives ofte av et brennende engasjement og er non-profit. Dette gir denne typen organisasjon en uavhengighet og en «stå-på vilje» som kan gjøre disse organisasjonene mektige. Disse vil «overvåke» de offentlige instansene, og kommunisere med publikum.

Datatilsynet vil være underlagt kontroll spesielt fra JSA som det rapporteres til. Datatilsynet vil igjen føre kontroll med Kripos. Både Datatilsynet og Kripos vil rapportere til overstående ledd i kontrollprosessen; enten ved at man svarer på «tiltale» eller på eget initiativ. Kontrollaspektet er likevel ovenfra- og ned jfr. modellen.

I de fleste tilfeller vil nok folk flest bli opplyst via media om aktuelle saker, da gjerne med Datatilsynet som fronter sine synspunkter. Dette kan sies å fungere i en slags vekselvirkning. En privatperson kan også gå direkte til mediene. Publikum vil kunne være i kontakt med Datatilsynet, og Kripos. Sistnevnte er nok heller uvanlig, da Kripos i sitt arbeide vil føre kontroll med allmennheten. Hvorfor allmennheten ikke har noe særlig kontrollevne overfor Kripos vil også her bli vist.

5.2 Kripos – på innsiden av systemet

Siden mye av litteraturen rundt SIS har et utenfra- og inn perspektiv har det vært svært viktig for avhandlingen å få kontakt med ”innsiden” og brukerne av systemet. Mine to informanter i Kripos har vært med fra begynnelsen når systemet ble implementert og har førstehåndskunnskap til hele prosessen.

Det meste av litteratur på feltet går på ren kritikk rettet mot SIS uten å slippe innsiden av systemet til. Dagens politiarbeid har også en stor grad av hemmelighold over seg, som gjør at det er vanskelig for forskere å få adgang på innsiden av «overvåkingsmuren» hos politiet (Sheptycki, 2007). Dette bidrar til å holde systemene og overvåkingen skjult.

I Norge er det Kripos ved SIRENE-kontoret som er Norges representant for politisamarbeidet i Schengen. Lov om Schengen informasjonssystem beskriver ansvaret til Kripos:

> *«Den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet (Kripos) skal føre et register som er den norske delen av SIS. Registeret skal kommunisere med det sentrale system og inneholde meldinger som er lagt inn av norske myndigheter. Kripos er registeransvarlig, og skal bl.a. sørge for at opplysninger som legges inn av norske myndigheter i SIS, er korrekte, oppdaterte og registrert på lovlig måte».*(Endringslov til SIS-loven § 2).

Kripos vil således kontrollere og kvalitetssikre informasjon som går ut fra Norge og fungere som et knutepunkt mot samarbeidende parter i andre Schengenland.

Det avholdes opplæringskurs for saksbehandlere både i regi av Kripos og EU ved CEPOL (European Police College). For å sikre at flest mulig deltar i informasjons- og opplæringssekvenser avholdes det i tillegg «webinarer»[3].
En del av kritikken som har vært rettet mot SIS er at det eksisterer store forskjeller på bruk og praksis i systemene. De overnevnte opplæringstiltakene har det vært rettet lite oppmerksomhet rundt og kan bidra til å utjevne eventuelle forskjeller mellom landene.

Ved SIRENE-kontoret har man ansatte som behersker en rekke språk; blant annet spansk, italiensk og rumensk. Dette kan bidra til at kontorene seg i mellom kan kommunisere enklere og mer effektivt, samt at det kan forhindre feilkilder. Dette kan nok bidra til å bedre personers rettssikkerhet, slik at man forhindrer feilføringer og feilkommunikasjon. Mine informanter ser også viktigheten av å ha gode kontakter i utlandet og å skape seg et nettverk. Dette kan imidlertid reise spørsmål om hva det kan føre til at noen land har bedre nettverk enn andre. Kan det føre til at utveksling av informasjon mellom visse land går lettere fordi man har gode kontakter, men at det kan være vanskeligere for andre? I et slikt «kaldt» og teknisk system som SIS utgir seg for å være skulle man ikke tro at nettverksbygging skulle spille noen rolle, og det er til dels urovekkende om det så er tilfellet.

Mine representanter i Kripos gir uttrykk for at landskapet de arbeider i er lovregulert, som ikke gir rom for fortolkning. Schengenkonvensjonen legger føringene for arbeidet. Kontorene må forholde seg til SIRENE-manualen, og det er viktig at man forholder seg til denne på en lik måte. Jeg innvender at det kanskje er en mulighet for at landene kan tolke denne forskjellig fra hverandre. Mine informanter meddeler at det er et bra regelverk som er enkelt

[3] Nettbaserte seminarer.

og greit å forholde seg til, og man har også interne rutiner og retningslinjer i Kripos i tillegg. De opplever ikke ulik praksis i sitt daglige arbeid. Men dersom det er slik at alle enheter som arbeider med SIS har sine egne rutiner og retningslinjer kan dette i seg selv gi rom for ulikhet. Samtidig er man avhengig av dette for å kunne gjennomføre arbeidet ved en arbeidsplass. For en utenforstående vil det ikke være mulig å få direkte innsyn i rutinene og retningslinjene, og vil dermed heller ikke ha mulighet til å kartlegge dette landene i mellom. Dette blir derfor bare basert på generelle betraktninger.

I SIS registreres søkbar informasjon og det er klare bestemmelser for hva som kan registreres. Informasjonsutvekslingen er bilateral og går direkte mellom kontorene via et sikkert nettverk. Man fyller ut forhåndsdefinerte skjemaer når man forespør informasjon – dette reguleres også av Schengenkonvensjonen. Systemet er strengt basert på koderegistreringer, og det er ikke rom for fritekst. Det er et "hit/-no hit" system, enten får man treff eller ei. Det er ikke et etterretningssystem, og behandlingen er formålsbestemt. De understreker at man er *formidlere av informasjon*. Når det gjelder muntlig kommunikasjon skulle man kanskje tro at dette gjelder spesielt i saker som haster, men det er ikke tilfellet. Man får en bekreftelse på mottak av info, skriftlig i all hovedsak. Et treff i systemet vil utløse en bestemt saksbehandlerprosedyre som vil utføres i tråd med SIRENE-manualen. Som mine informanter understreker er det så klare regler at det å fravike disse er vanskelig.

Mye av litteraturen beskriver at mange instanser i andre land, flere enn i Norge, har tilgang. I Norge har politiet, og snart også tollvesenet og vegmyndighetene tilgang til SIS. Det er uvisst når tilgangen til disse blir gitt, men det er besluttet. UDI har også tilgang til deler av systemet, men det er kun den delen som går på innreisenekt for tredjelandsborgere, altså ikke det totale systemet (Schengenkonvensjonen, 2007 art.96). På bakgrunn av dette er det store forskjeller mellom Norge og de andre Schengenlandene. Hvilke organer som skal ha tilgang er riktignok regulert, men i skrivende stund er det uheldige forskjeller som gjør at Norge blir hengende litt etter.

Mine informanter understreker at man er en del av et stort internasjonalt system, og man har fått et ansvar. Alle har fått oppgaver som følge av Schengen; Kripos, Datatilsynet og UDI.

Mine informanter i Kripos bekreftet i min samtale med dem at Datatilsynet holder tilsyn hos Kripos, og at tilsynet kan være både varslet og uvarslet. De kontrollerer at behandlingen av data utføres i henhold til de ulike artikkeltypene. Kripos understreker at personvern er en

viktig del av SIS-loven. Mine informanter i Kripos meddeler at det gjennomføres en kvalitetssikring av opplysninger som går ut fra Norge. Man har også i dette henseendet Schengen-inspeksjonen som består av representanter fra EU der ulike land reiser rundt og fører kontroll. Representanter fra Norge kan også bli valgt ut til dette kontrollarbeidet. Hensikten er å kontrollere at medlemslandene oppfyller sine forpliktelser i henhold til regelverket.

Mine informanter understreker at man har retningslinjer for bruk av systemet. Dette er et faktasystem og ikke et etterretningssystem, og man kan ikke etterlyse en person uten å ha hjemmel til det. Schengenkonvensjonen legger føringene. Det er også saneringsregler for når informasjon skal fjernes fra SIS.

5.2.1 Overvåkingssystem eller informasjonssystem?

Det å studere hva slags begreper som benyttes om et fenomen er interessant. Det kan fortelle noe om hva slags holdninger som ligger bak, og om det er noe man ønsker å skjule og glatte over. Et godt eksempel som aldri slutter å fascinere er begrepet som benyttes om fengselssystemet i Norge; «kriminalomsorgen». Det taler for seg.

Litteraturen på feltet omtaler SIS som et *overvåkingssystem*. Dette kan vise seg å være et definisjonsspørsmål. Det er interessant at ens ståsted påvirker hvordan en velger å omtale systemet.

Mine informanter i Kripos stiller seg uforstående til at jeg i forbindelse med deres arbeid benytter begrep som ”overvåking” og ”overvåkingssystem”. Jeg får beskjed om heller å fokusere på ”informasjonssystem” da dette er snakk om et fakta-register. Det er mulig ”overvåking” oppfattes som et negativt ladet uttrykk – de identifiserer seg ikke med dette begrepet. En av mine andre informanter mener i likhet med Kripos at det er feilaktig å se på SIS som et overvåkingssystem, og at *etterlysningssystem* er et mer passende begrep.

> *«Nei, SIS er et etterlysningssystem. Det er jo sånn sett et overvåkingssystem for de registrerte, men det er andre mekanismer vi tradisjonelt vil se som et overvåkingssystem. Jeg vil nok legge andre tiltak i kategorien overvåking. Det er begrepsdefinisjoner sånn sett. Det kan hende Kripos ikke ville kalle det det».*

Et par av mine informanter understreker at det er forskjell på informasjon og overvåking. Når man begynner å tolke informasjon og stiller spørsmål som; hvem er denne personen? Hvor skal hun hen? Da er man over på overvåking og intelligens. Det er legitimt å mene at dersom informasjonen skal ha en funksjon må den også tolkes og benyttes til noe. På denne måten vil det nok være for lett å avfeie «overvåking» som et begrep som ikke her bør benyttes. Nå er riktignok litteraturen på feltet også av mer kritisk karakter som selvsagt vil beskrive systemet deretter. Det er et definisjonsspørsmål.

Det kan imidlertid legges til at begrep som «*surveillance*» og «*discreet surveillance*» går igjen flere steder i Schengenkonvensjonen.

5.3 Datatilsynet som kontrollinstans

Det har vært viktig å oppnå kontakt med Datatilsynet, siden Datatilsynet er den instansen i Norge som fører tilsyn med Schengen Informasjonssystem i Norge. Datatilsynet har det overordnede ansvaret for å påse at retningslinjene med hensyn til personvern, bruk og datasikkerhet blir overholdt. Datatilsynet har på denne måten en tilsynsrolle, men også en ombudsrolle der de kan komme med innspill til utvikling av regelverket. Som beskrevet tidligere blir SIS ansett som et kompenserende tiltak når grensekontrollen er bygget ned. Men det føres også kontroll med kontrollørene. Datatilsynet er denne kontrolløren i Norge. Datatilsynets rolle beskrives i SIS-loven:

> *«Datatilsynet skal kontrollere at loven og forskrifter gitt i medhold av loven blir fulgt, og at feil eller mangler blir rettet. Datatilsynet skal etter begjæring fra den registrerte kontrollere om opplysningene om vedkommende i SIS er riktige, om reglene om innsyn er fulgt, og om opplysningene er registrert og brukt i samsvar med denne loven. Dersom opplysningene er lagt inn av en annen konvensjonspart, skal kontrollen foretas i samråd med denne konvensjonspartens kontrollorgan»* (Endringslov til SIS-loven § 21).

Georg Apenes var leder for Datatilsynet da Norge underskrev Schengen-avtalen i 2001 og dette er også årsaken til at det har vært viktig å oppnå kontakt med han.

Apenes gir uttrykk for at Datatilsynet ikke var særlig engasjert i utrullingen av systemene når Norge gikk inn i Schengen. Datatilsynet var ikke delaktig i den tekniske tilretteleggingen, det var først senere de kom på banen.

> *«Vi kom jo til duk og dekket bord og ting var jo enten take it eller leave it. Flere og flere meldte seg jo inn og Norge var av de siste. Og vi ble ikke spurt om hva vi mente om de kontrollmekanismene og kontrollmetodene som Schengen akkorden skulle lyde på».*

Det gis uttrykk for at Datatilsynet ikke ble involvert og heller ikke hadde noe kontakt med Kripos i denne perioden angående SIS, hverken på utformings- eller tilsynssiden. Det gis også uttrykk for at siden Norge kom så sent inn og de andre landene allerede hadde innført systemene var det lite Norge kunne påvirke. Tilsynsrutinene har altså kommet til i ettertid. Dette vil i større grad bli tatt opp senere der jeg ser på tendensen til at man tar opp personvern som tema først når ballen har begynt å rulle.

5.3.1 Datatilsynet; kontroll og innsynsrett

Min informant hos dagens Datatilsyn ved tilsynsavdelingen bidrar til å forklare hvordan tilsynsordningen fungerer i dag. Det blir raskt gjort klart for meg at inspeksjonen Datatilsynet gjør hos Kripos har *The Joint Supervisory Authority of Schengen* (JSA) i ryggen.

JSA er et uavhengig organ som består av medlemmer fra de ulike lands kontrollører av datasikkerhet (The Joint Supervisory Authority of Schengen, 2013 2.2.2013). De nasjonale ekspertene som utgjør revisjonsteamet er i følge min informant rullerende, og Norge har tidligere blitt utvalgt til å delta. Deres oppgave består blant annet i å kontrollere at Schengenkonvensjonen overholdes, og kontrollerer de nasjonale enhetene som fører kontroll med bruken av SIS – i Norges tilfelle Datatilsynet. JSA bidrar også til å identifisere eventuelle problemer som måtte oppstå i bruken av SIS og kommer med problemløsende forslag. JSA har sitt sekretariat situert i Brussel (The Joint Supervisory Authority of Schengen, 2013 2.2.2013).

JSA følger opp Datatilsynet, og inspiserer at det norske Datatilsynet utfører sin oppgave på riktig måte. Sist gang Datatilsynet i Norge ble kontrollert av JSA var i oktober 2011 der vi ble revidert som nasjon. I en slik kontroll blir det gjennomgått hvordan Datatilsynet følger opp sin kontrollrolle overfor Kripos og de andre partene, eksempelvis UDI. Min informant kan fortelle at Datatilsynet har lite kontakt med EDPS, men møter dem i internasjonale sammenhenger.

På tilsynsavdelingen hos Datatilsynet er det 11 saksbehandlere; 3 samfunnsvitere, en jurist og 7 teknologer. Teknologene skal ha ulike spesialområder; informasjonssikkerhet og teknologi som telecom, applikasjoner («apper») og liknende. Dette for å kunne ha mulighet til å følge teknologiutviklingen. Min informant meddeler at deres arbeid i praksis ikke bare omhandler Kripos, men at Kripos utgjør en *stor del* av deres totale arbeidsmengde. JSA sender tidvis spørreskjemaer som Datatilsynet vil føre kontroll etter. I 2009 ble det gjort kontroll på et spørreskjema knyttet til artikkel 97 og 98 som gjelder de ulike registreringsvilkårene i SIS.

I tillegg til å utøve kontroll med Kripos er Datatilsynet også instansen i klagesaksbehandling. Dersom man blir nektet innsyn i opplysninger i SIS havner disse klagesakene på Datatilsynets bord. Kripos mottar om lag 10 begjæringer om innsyn i SIS årlig og Kripos mener dette indikerer at det ikke er mange situasjoner som utløser et ønske om innsyn (Kripos, 2011). Som vil bli vist senere er offentligheten i stor grad avhengig av at media viser interesse for å bli informert og dermed engasjert. Datalagringsdirektivet er et godt eksempel på at folks engasjement har blomstret opp på grunn av medias innsats.

> *«Vi er jo tilsynsmyndighet etter SIS-lover og SIS-forskrifter. Day-to-day samarbeidet er begrenset, skal være begrenset. Vi skal ikke delta i saksbehandlingen. Vi er eventuelt en klageinstans. Det vil være i de tilfeller der Kripos, eventuelt via distrikter får innsynsforespørsel, får klage på det, får et avslag. Det blir klaget – Kripos velger og ikke omgjøre det på egenhånd og det går opp til oss. Da vil vi kunne uttale oss der. Vi har en rolle i klagesaksbehandling.»*

SIS er et system som opererer litt i gråsonen når det gjelder innsyn. I utgangspunktet skal man ha rett til innsyn i SIS, og også få endret uriktige opplysninger (Mathiesen, 2000). Dette er lovfestet i *offentlighetsprinsippet* (Ny offentlighetslov, 2003:30). Allikevel finnes det unntak fra dette. Selv om kravet til innsyn også nevnes i Schengenkonvensjonen (2007) art.109 overlates det til de ulike nasjoners lover på området for å avgjøre hva som skal være gjeldende rett. På bakgrunn av dette kan det tenkes det vil være noe variabel praksis i de ulike statene. Dette vil si at rettssikkerheten til personer i stor grad vil avhenge av hvilket land man befinner seg i. I tillegg kan et vedtak om innsyn fattes på bakgrunn av skjønnsvurderinger.

> *«(…)*Kapittel 2 *gjør en rekke unntak fra konsesjonsplikten etter personregisterloven § 9. Det er knyttet en rekke vilkår til disse konsesjonsfritakene; bestemmelser om registrenes innhold, bruk mv (*kapittel 2 *og* 3*)».* (Et bedre personvern, NOU 1997:19).

Dette betyr i praksis at dersom innsyn i opplysninger vil stå til hinder for formålet, eksempelvis en etterforskning, vil innsyn kunne nektes (Mathiesen, 2000). Det vil også ha noe

å si hvilken «fase» opplysningene er i; skal de brukes for en etterforskning holdes de skjult, mens eldre opplysninger kanskje mister litt av sin verdi for politiet og er trolig lettere å få tilgang på.

> *«Den registrerte har rett til å få opplyst hvilke opplysninger om seg selv som er registrert i SIS. Den registrerte kan ikke få innsyn i opplysninger dersom det kan skade gjennomføringen av det tiltaket det er anmodet om, eller dersom vernet av andre personer tilsier det. Innsyn skal alltid nektes i det tidsrommet det er anmodet om observasjon. Begjæring om innsyn fremsettes for den registeransvarlige eller den myndighet som har besluttet registrering, men avgjøres av den registeransvarlige. Dersom meldingen det begjæres innsyn i, er lagt inn av en annen konvensjonspart, plikter den registeransvarlige å gi denne konvensjonsparten anledning til å uttale seg før innsyn gis».* (SIS-loven § 15).

Dette bekreftes også i min samtale med Datatilsynet som har hatt noen få klagesaker på grunn av avslag på forespørsel om innsyn. Generelt er politiets arbeidsregistre unntatt registerinnsyn (Mathiesen, 2000).

> *IO: «(...) du har rett på innsyn på hva som er registrert om deg, og om du er registrert. Og i sakens natur så er det ikke all informasjon du skal ha rett til innsyn i, om du er ettersøkt for eksempel, etterlysningskategorier hvor det skal gå en varsling, men ikke en pågripelse. Naturlignok skal man ikke ha informasjon om at man er registrert ved en sånn registrering».*
>
> *I: «Hvis jeg som privatperson hadde tatt kontakt med Kripos, ville jeg fått utlevert opplysningene om meg?»*
>
> *IO: «Hvis det var opplysninger i SIS om deg, og du ba om innsyn, så er det ikke sikkert at du ville fått de. Og da vil de i så fall gi et avslag på innsynsforespørselen. Og så er det jo regulert i hvilke tilfelle de kan gi avslag eller nekte innsyn».*

Sannsynligheten er også liten for at en som er ettersøkt vil melde seg for innsyn i egne opplysninger. I mange tilfeller er man heller ikke klar over at man befinner seg i registrene. Min informant nevner at Datatilsynet kun har hatt to-tre saker knyttet til innsyn eller sletting av opplysninger i SIS, noe som må sies å være et lite antall. Man har heller ikke funnet noen brudd på regelverket for SIS i dette henseendet.

5.4 Datatilsynets kontrollrapport 2012

Datatilsynet vil føre kontroll med Kripos og deres arbeid knyttet til SIS, tilsynet utføres etter SIS-loven og SIS-forskriftene. Kontrollen kan variere både med hensyn til om man tar en stedlig kontroll eller ber om en skriftlig redegjørelse, og om kontrollen er varslet eller uvarslet. Datatilsynet i Norge vil intervjue, se på dokumentasjon, samt se på hvilke tiltak Kripos selv har gjort i dette arbeidet.

I juni 2010 gjennomførte Datatilsynet et stedlig tilsyn der det ble sett på de systematiske pliktene og sikkerhetsarbeidet knyttet til SIS. Kontrollen gikk på å se på om det var utarbeidet en god nok internkontroll hos Kripos. Det ble i tillegg utført en kontroll på en grensestasjon i Østfold ved Rygge flyplass med politiet som bruker samt ved Vansjø lensmannskontor (Datatilsynet, 2012). Tollmyndighetene i Norge har som nevnt foreløpig ikke tilgang til SIS. Jeg har fått tilgang til rapporten samt brevkorrespondansen mellom Datatilsynet og Kripos i etterkant av tilsynet i en sladdet versjon. Datatilsynet påpeker en del forhold av teknisk og administrativ art som det her vil bli gått nærmere inn på. Dette er avgjørende for å forstå hvor dagens utfordringer og forbedringspotensial i praksis ligger samt gi det hele en mer konkret forankring.

5.4.1 Uklar ansvarsfordeling

Rapporten tar for seg de tekniske og administrative forholdene knyttet til bruken av SIS, og systemets sikkerhetsmessige ivaretakelse. Et av de største ankepunktene i rapporten er at det hersker en uklarhet i Kripos sitt ansvarsforhold overfor politidistriktene og UDI (Datatilsynet, 2012). Dette var ikke dokumentert, og det fremstod som uklart om det var Kripos sin oppgave å følge opp at regelverket ble overholdt i de andre brukerinstansene (Datatilsynet, 2012). I Kripos' brev til Datatilsynet går det frem:

> *«Det bemerkes i denne sammenheng at Kripos årlig kontrollerer at distriktene har foretatt en gjennomgang av autorisasjoner og brukerroller i ELYS II, herunder tilgang til SIS gjennom ELYS II-applikasjonen. Det er korrekt at det ikke eksisterte en systematisk oppfølging på tilsynstidspunktet (…). Spørsmålsstillingen ble på dette punktet trolig noe misforstått under*

> *tilsynet. (…) Det stemmer at Kripos har igangsatt et arbeid for etablering av styringssystem basert på ISO 27000-serien*[4]*»* (Kripos, 2011).

Kripos har også utarbeidet en instruks for politiet og UDI med kvalifikasjonskrav til de som bemyndiges tilgang til SIS (Kripos, 2011). Det går også klart frem at myndigheten til Kripos er noe begrenset og at det finnes flere inngangsporter til SIS enn jeg først antok:

> *«Søk og registrering i SIS fra UDI foretas via UDI's egne fagapplikasjoner DUF og Norvis, og gjøres kun i forbindelse med saksbehandling og fatting av vedtak innenfor UDI's ansvarsområde. Kripos har eksempelvis ikke myndighet til å kontrollere grunnlaget for en innmelding i SIS foretatt av UDI etter artikkel 96 i Schengenkonvensjonen jfr. SIS-loven § 7 nr. 2. På dette området har UDI et selvstendig ansvar for egne behandlinger»* (Kripos, 2011).

Det samme gjelder oppfølging av loggingen. Det var uklart for Kripos om de hadde ansvar for sikkerhetstiltak knyttet til UDI's bruk av systemet (Datatilsynet, 2012).

> *«Den registeransvarlige skal etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven. Den registeransvarlige skal dokumentere tiltakene. Dokumentasjonen skal gjøres tilgjengelig for medarbeiderne hos den registeransvarlige og dennes databehandler. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda»* (SIS-loven, § 4).

En del av diskusjonen går også på i hvilken grad UDI skal anses som en databehandler (Kripos, 2011).

I henhold til loven er dokumentasjonen knyttet til ansvarsområde mangelfull (Datatilsynet, 2012). Men i følge brev fra Kripos (2011) til Datatilsynet anses ikke dette som en potensiell konfliktsituasjon slik Datatilsynet fremstiller saken.

Det som trekkes frem i rapporten som en kompliserende faktor er at Kripos er underlagt Politidirektoratet på lik linje med politidistriktene, og Kripos har i utgangspunktet ingen instruksjonsmyndighet overfor distriktene (Datatilsynet, 2012). Det ble av Kripos uttrykt misnøye med situasjonen, og det var uklart også for dem hvilke myndighet de har overfor de andre instansene (Datatilsynet, 2012).
Datatilsynet mener Kripos har både *rett* og *plikt* til å instruere politidistriktene og UDI (Datatilsynet, 2012). Det understrekes at det er helt avgjørende at ansvaret for registrene og myndigheten tillegges samme organ. Ut i fra kravet om internkontroll i SIS-lovens § 4 anses dette i følge rapporten som et avvik da det er uklarheter i ansvarsforholdene. Det ble også

[4] ISO (International Organization for Standardization) - standard for informasjonssikkerhet (www.iso.org 2.2.2013).

påpekt at kontrollen med om de fastsatte rutinene og regelverket ble fulgt opp ikke var tilstrekkelig og på daværende tidspunkt var ikke avvikshåndteringssystemet operativt (Datatilsynet, 2012). Dette vil også gå inn under § 4 i SIS-loven.

Ved Moss lufthavn kom det frem under kontrollen at materialet politiet hadde fått tildelt fremsto som fragmentert da det for samme tjenesteområdet var utstedt materiale både av Kripos og Politidirektoratet (Datatilsynet, 2012). Dette kan føre til ulik instruks, og det er nærliggende å anta at Kripos er den beste kandidaten til å utarbeide denne type materiell. Allikevel fant politiet på Rygge både rutinene og instruks dekkende for å kunne gjennomføre tjenesten (Datatilsynet, 2012).

5.4.2 Tekniske utfordringer

Et viktig punkt på Datatilsynets agenda har i følge min informant vært å sikre god logging og logganalyse i systemene. I rapporten beskrives det at Datatilsynet ba om å få de siste 100 oppslagene som var foretatt i SIS fremlagt fra Kripos (Datatilsynet, 2012). Dette måtte klargjøres i en særskilt prosess, og loggene fremstod som utilgjengelige. Kripos opplyste riktignok at dette skulle implementeres når et nytt avvikssystem kom på plass i den såkalte «Kriposnøkkelen». I loggene kunne man heller ikke få frem informasjon som kunne knytte søk til identitet eller lokasjon, hverken geografisk eller administrativt (Datatilsynet, 2012).

Logganalyse i ettertid er avgjørende. Min informant understreker at den «flate» loggen ikke fungerer i seg selv i praksis - for at en logg skal ha en funksjon må den analyseres og dette gjøres først når man har mistanke om at det er noe galt eller har en konkret klage. Man må analysere loggene og gjøre en god loggkontroll. Det var riktignok etablert logging med tanke på moderne fagsystemer, men det fantes utfordringer med de eldre fagsystemene. Det blir gjort klart for meg at det i praksis er tre trinn hvor man har grenseflater som brukeren sitter på; polititjenestemenn som bruker systemet til søk, det nasjonale systemet og det internasjonale systemet. Spørsmålet er hvor man skal legge loggingen når man har tre mulige plasseringer. Eksempelvis på det norske systemet der man bare registrerer en maskinforespørsel så vil ikke det fortelle noe om identiteten til den som gjorde oppslaget. Datatilsynet fant imidlertid at Kripos tenkte godt og riktig med hensyn til dette i det moderne

systemet. En annen problemstilling som ble reist var i hvilken grad Kripos er pliktet til å sikre logging for UDI som har tilgang til deler av systemet, dette er igjen knyttet til ansvarsfordelingen. Det kan her legges til at det i Schengenkonvensjonen (2007) art.103 kreves at hver overføring av personlig data skal loggføres slik at man kan kontrollere at det er blitt utført med tillatelse.

Risikovurderingene var også mangelfulle. Min informant forklarer at det er avgjørende at man setter opp et styringssystem for informasjonssikkerhet, altså en ramme for bruk av systemet. Man skal sørge for opplæring, sørge for kontroll med og om regler man selv har satt blir fulgt i praksis. Når det gjelder risikovurderinger vil det bestå i at man vurderer hva som kan gå galt og sikrer systemet ut i fra dette. Det ble ansett som et avvik knyttet til sikkerhetsledelse og risikovurderinger at det ikke var etablert tiltak for å sikre informasjonssikkerheten. Kripos hadde likevel iverksatt noen tiltak for å utbedre situasjonen uavhengig av kontrollen. Kripos understreker i sitt brev til Datatilsynet at de har iverksatt omfattende kvalitetssystemer som består av Kriposnøkkelen (prosessdiagrammer), EK Kriposbibliotek og Delta avvikssystem (Kripos, 2011).

Det ble også funnet avvik på § 7-7 med hensyn til konfigurasjonskontroll. Det viste seg å være lite kontroll med hvilke applikasjoner som gir tilgang til SIS, blant annet en applikasjon som skal fases ut (N-SIS)[5].

I følge Kripos går opplysninger fra Norge ut via et sikkert datasystem, og jeg var spørrende til om Datatilsynet har tatt stilling til sikkerheten på dette systemet. Det blir fortalt at det ikke har blitt observert noen særskilte utfordringer knyttet til det og at det også har blitt fulgt opp av JSA. Når man gikk inn på Schengen-infrastrukturen så har det ikke vært knyttet bekymringer til dette, men spørsmålet er vel snarere om det har blitt ført særlig kontroll med dette og hvem som egentlig har ansvaret. Det kan se ut til at det her er et lite hull i «kontroll-veggen». Dette kan knyttes opp mot globalisering – spørsmålet kan reises om det fanges opp av noen der Datatilsynet slipper taket.

> *«Vi har heller ikke gått inn og vurdert det eksplisitt, og vi har heller ikke vurdert hvor starter og slutter kompetansen vår knyttet til den internasjonale infrastrukturen. Jeg er kanskje spørrende til om vi har kompetanse på det som foregår der».*

[5] N-SIS er en tidligere applikasjon for bruk av SIS. Kan ikke lengre brukes til å gjøre registreringer.

Kripos understreker at flere av punktene som påpekes under tilsynet vil avhenge av et større avklaringsarbeid i politiet og justissektoren for øvrig, men at noe av det som påpekes i *«større eller mindre grad var på plass allerede på tilsynstidspunktet»* (Kripos, 2011). Det understrekes også at det er nedsatt flere arbeidsgrupper hos Kripos som vil påvirke behandlingen av personopplysninger der man skal arbeide med et helhetlig internkontrollsystem. Her vil det bli arbeidet med å utarbeide juridisk styrende dokumenter for ivaretakelse av Kripos behandlingsansvar og informasjonssikkerhet. Kripos formidler at dette vil føre til økt personvernfokus i politiet, men understreker samtidig følgende:

> *«Kripos ber om aksept for at dette mer helhetlige arbeidet, som jo i stor grad vil medføre økt personvernfokus i politiet, må gå sin naturlige gang i stedet for at det igangsettes hastverksarbeid på ett enkeltområde som SIS»* (Kripos, 2011).

Kripos nevner også at grunnet kort tidsfrist før kontrollen kan dette ha medført at de faktiske forholdene ikke ble belyst tilstrekkelig (Kripos, 2011). De mener også at noen forhold ikke har blitt tilfredsstillende belyst fordi tilsynet ble varslet på så kort tid at Kripos fikk problemer med å innkalle nødvendig personell.

Jobben til Datatilsynet går altså i stor grad ut på å kontrollere hvordan Kripos selv ivaretar oppfølgingen med hensyn til kvalitet og informasjonssikkerhet i bruken av systemet. Det blir i intervjuet gjort klart for meg at praksisen fra de ulike tilsynsmyndighetene varierer noe internasjonalt. Noen vil sette seg ned og gjennomføre en loggkontroll med politiet. Men det er Kripos selv som skal bygge systemet og sørge for at regelverket følges. Min informant i Datatilsynet er klar på hva som er deres ansvarsområde.

> *«Vi gidder ikke pakke inn at vi mener at det er ikke vår jobb i det hele tatt. Vår jobb er å kontrollere at politiet selv har gode nok rutiner; god nok teknisk logging og god nok rutine for å gå i gjennom loggene. Vi skal sjekke at deres kontrollrutiner fungerer, for det er dem som er pliktet til å sikre dataene. Vi skal ikke gå inn og gjøre et informasjonssikkerhetsarbeid hos dem. Det vil være en forskjellig tilnærming. Vi har en del DPA's (data protection authoritys) som kommer rullende med logganalyseverktøy og går i gang og gjør den type analyse. Men vi kontrollerer; gjør de jobben sin selv?»*

Datatilsynet fant at det var utfordringer knyttet til systemet, men en del av dette har latt seg løse etter kontrollen. Det legges til fra min informant at dette er utfordringer man møter i implementeringen.

> *I: «Så det er ikke verre forhold hos Kripos enn hos andre steder der dere gjør tilsyn?»*
>
> *IO: «Nei, men klart, dette er jo veldig inngripende opplysninger. Og så har politiet også mye annen informasjon. Det er sånn sett et fåtall registrerte her, hvor du da gjør konkrete søk på person og kan få et treff. Det er jo også andre system i politiet, nødvendig sådan for at politiet skal kunne gjøre jobben sin, som nok også representerer et større misbrukspotensial knyttet til personverndelen. Jeg vet ikke hvor mange treff du kan få, men befolkningen i registrene er jo vesentlig større i en del andre, STRASAK og politilogg og liknende».*

Selv om SIS kanskje ikke er så utsatt som de andre informasjonssystemene i politiet isolert sett vil SIS skille seg kraftig ut ved at opplysningene forlater landet og kan gjøres tilgjengelig for 25 andre land, og data kan også ende opp i samarbeidende registre. Slik sett vil potensialet for at data i SIS utsettes for misbruk totalt sett være større med alt det dette innebærer.

Jevnt over får jeg inntrykk av at kontrollen Datatilsynet har med SIS i Norge er god. Kunnskapen og de punktene som har blitt påpekt vitner om god detaljinnsikt i SIS og høy grad av faglig forståelse. Om kontrollen med SIS er like god fra datatilsynene i andre land vil kreve en større kartlegging.

5.5 Andre Schengenrelevante kontrollorganer

Selv om Datatilsynet i Norge er den instansen som hovedsakelig vil være kontrolløren av SIS finnes det også andre instanser innenfor EU som har kontrolloppgaver i kontrollmaskineriet. Det kan være fristende å benytte «stjernedryss»-betegnelsen også her for å beskrive omfanget, selv om det finnes langt flere overvåkings- og kontrollorganer enn det finnes instanser som påser at datasikkerhet og personvern ivaretas. De er mange, men de fleste tar for seg bare en liten del av et stort hele. Jeg vil her gi en beskrivelse av de to største internasjonale instansene og en forklaring på deres kontrollbrikke i dette lappeteppet av overvåkingsinstanser.

5.5.1 European Data Protection Supervisor (EDPS)

European Data Protection Supervisor (EDPS) er et kontrollorgan situert i Brussel. Deres oppgave er å påse at alle organer innenfor EU forholder seg til gjeldende regler for personvern

ved behandling av data og når det etableres nye retningslinjer. EDPS har også en rådgivende rolle og yter bistand i forbindelse med spørsmål knyttet til databeskyttelse og personvern. Man kan som nasjon kontakte EDPS for å få rådgivning knyttet til spørsmål rundt overnevnte temaer.

Rent administrativt har EDPS to ledere (supervisors); Peter Hustinx (leder) og Giovanni Buttarelli. Disse er EDPS' ansikt utad. Kontoret har omkring 40 ansatte fordelt på fem sektorer; *politician consultation unit, supervision and inforcement unit, information and communication, operational support unit* og *HR and administration*. Min informant er utdannet jurist og arbeider i den største avdelingen; politician consultation unit. Denne avdelingen har en rådgivende funksjon knyttet til beskyttelse og behandling av persondata i EU's organer.

Mine informanter som har hatt kjennskap til EDPS og deres virksomhetsområde har tatt det for gitt at SIS er underlagt kontroll fra EDPS. Det var først i min samtale med EDPS det kom frem at SIS ikke er underlagt noen som helst kontroll fra EDPS på nåværende tidspunkt. Det er *The Joint Supervisory Authority of Schengen (JSA)* som sitter med dette ansvaret.

Nye arbeidsoppgaver for EDPS

Når SIS II nå lanseres vil det skje et skifte i kontrollen av SIS. EDPS kommer til å overta ansvaret som kontrollerende autoritet. For det første har EDPS hittil hatt lite med SIS å gjøre, det samme gjelder for SIRENE som heller ikke er underlagt EDPS. På bakgrunn av dette mener min informant i EDPS at hverken han eller noen andre i EDPS er kompetente til å uttale seg i større grad om SIS, men kan uttale seg på generelt grunnlag.

For det andre er det noe merkverdig at et så sentralt organ med hensyn til personvern i Europa ikke har hatt noe med SIS å gjøre til nå. Det er også grunn til å tenke over det faktum at EDPS kommer til å overta hele ansvaret for systemet når det til og med er i ferd med å vokse seg enda større og mer omfattende enn slik det fremstår i dag. De vil på bakgrunn av dette heller ikke sitte på verdifulle erfaringer som nok kunne komme godt med i arbeidet med å holde dette systemet i «tøylene».
På en annen side kan det muligens bringe med seg noe positivt at et organ uten erfaring med

SIS kommer inn og ser systemet med friske øyne, samt at EDPS med personvern som kompetansefelt nok vil være meget godt egnet til denne oppgaven. Kanskje kan dette føre til at systemet kan gås litt etter i sømmene.

Man kan tenke seg at problemene som har vært skissert tidligere ikke vil bli mindre med tanke på at SIS II vil inneholde et større og mer komplekst datainnhold enn dagens SIS. Det kan på en annen side hjelpe at EDPS vil koordinere de nasjonale autoritetene.

EDPS har gått i gjennom forslagene til det nye SIS og i følge Parkin (2011a) ble deres meninger rundt systemet levert i det høyeste tempoet man har sett fra EDPS noen gang. Parkin innvender at det er grunn til å mene at SIS' skifte av natur med dets nye funksjonalitet ikke har blitt sett nøye nok i gjennom med tanke på individers rettssikkerhet som er en svært sentral del av et slikt system. Det er også rettet kritikk mot at det kun er et fåtall av personer som har stått for utformingen av hele systemet i likhet med dagens SIS (Parkin, 2011a).

5.5.2 The Joint Supervisory Authority of Schengen (JSA)

Det er flere såkalte «joint supervisory bodies», eller «kontrollorgan» i EU som alle har sine spesifikke ansvarsområder de fører kontroll med (www.edps.europa.eu, 2013b 6.3.2013). Det finnes egne kontrollorganer for Europol, Eurojust, toll og den mest relevante i denne sammenheng; *The Joint Supervisory Authority of Schengen* (JSA) som har det tekniske kontrollansvaret for SIS (edps.europa.eu, 2013b 6.3.2013). Det vil på bakgrunn av dette være interessant å se litt nærmere på JSA.

Som nevnt tidligere er JSA et organ som har til oppgave å påse at datasikkerheten ivaretas i Schengen (The Joint Supervisory Authority of Schengen, 2013 2.2.2013). 2 medlemmer fra de ulike landene vil kunne bli utvalgt til å delta da engasjementet i JSA er rullerende (The Joint Supervisory Authority of Schengen, 2013 2.2.2013). Det medfører riktighet å si at EDPS vil stå for de litt større linjene og har en rådgivende funksjon på et foreløpig overordnet nivå, mens JSA gjør større dypdykk i problematikk som er av direkte systemteknisk karakter når det gjelder SIS.

I motsetning til EDPS er JSA nevnt i Schengenkonvensjonen (2007) artikkel 115. JSA har sitt sekretariat i Brussel, men er av en noe mer «flytende» struktur og kanskje litt mindre

håndgripelig art enn EDPS. Dette skyldes nok til dels at kontrollgruppen ikke er nedsatt på fast basis. Hvordan denne utvelgelsen foregår er imidlertid også noe vanskelig å få tak på. Gruppen skal møtes minimum 2 ganger i året (The Joint Supervisory Authority of Schengen, 1996).

Kontrollen vil utføres på bakgrunn av Schengenkonvensjonens bestemmelser, men samtidig skal den nasjonale lov i hvert land også tas i betraktning (Schengenkonvensjonen, 2007 art.115). Hvordan dette løses rent praktisk er noe uvisst, men Schengenkonvensjonen nevner flere steder at det er de ulike medlemsstatenes lover man skal innrette seg etter. Dette kan settes i sammenheng med rettspluralisme som nevnt tidligere.

I tillegg til dette skal JSA også føre kontroll på bakgrunn av følgende:

> «*Supervision shall be carried out in accordance with (…) the Council of Europe Convention of 28. of January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data, taking into account Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector*». (Schengenkonvensjonen, 2007 art.115).

JSA skal ha tilgang til de tekniske supportfunksjonene for å kunne sikre at systemet er korrekt implementert, og har også ansvar for å identifisere eventuelle problemer knyttet til bruken av SIS. JSA har også rett til å bidra med løsningsforslag (Schengenkonvensjonen, 2007). JSA kan både på eget initiativ og på oppfordring fra et medlemsland sette i gang arbeidet i en medlemsstat (The Joint Supervisory Authority of Schengen, 1996).

Da kontrollfunksjonen er rullerende kan man selvsagt stille spørsmål ved de effekter dette kan bringe med seg. For uten å forsøke å komme med svar til dette reiser jeg likevel spørsmål knyttet til om denne rulleringsordningen kan bidra til «kontrollhull» ved mangel på kompetanse til forskjell fra hvordan situasjonen ville vært dersom JSA-kontrollørene bestod av et fastsatt team. Det overnevnte regelverk vil mest sannsynlig kreve både kunnskaper innenfor teknologi og jus. Det nevnes i «*Rules of Procedure of The Joint Supervisory Authority*» at man kan ha med seg eksperter på kontrollene (The Joint Supervisory Authority of Schengen, 1996). Det er heller ikke særlig hyppig møtevirksomhet, kravet er at gruppen møtes minimum to ganger i året. Man skal selvsagt heller ikke se vekk i fra muligheten for at det at kontrollfunksjonen er rullerende vil føre til en mer rettferdig kontrolløsning der alle land vil kunne ha lik sjanse for å bli utvalgt, økt ansvarsfølelse og kompetanseheving. Det er

også en mulighet for at stadig tilførsel av nye medlemmer vil kunne bidra til nye ideer som kan gi grobunn for diskusjon.

Det nevnes i reglementet at møtene som holdes ikke skal være offentlige (The Joint Supervisory Authority of Schengen, 1996). Dette er forståelig dersom det eksempelvis diskuteres sikkerhetstrusler og liknende som kan føre til at informasjon lekker ut, men det bidrar til at «sivilblikket» står igjen på utsiden.

Et noe interessant punkt er at JSA har skrevet deres regelverk selv, på bakgrunn av dette samt andre aktuelle saker har man fastsatt at «The General Secretariat of the Council» skal fungere som sekretariat for JSA og vil bistå på ulike områder (Council i Official Journal of The European Communities, 1999). Budsjettet til JSA er også en del i Schengen-budsjettet (Joint Supervisory Authority of Schengen, 1996). Kanskje ville en mer uavhengig instans vært et bedre alternativ?

JSA fremstår som litt mer skjult i terrenget enn EDPS. Fra et brukerperspektiv fremstår også deres nettsider som vil være første kontaktflate mot publikum som mindre informativ og brukervennlig enn nettsiden til EDPS. På nettsidene til EDPS kan man lese og se videoer som vil øke ens egen kunnskap og bevissthet rundt personvern, spesielt knyttet til Europa. Mest sannsynlig er dette området så lite kjent i utgangspunktet at det kanskje ikke er noe vits i å markedsføre et slikt særorgan i særlig grad, selv om det må kunne sees på som positivt at det eksisterer.

5.6 Har man god nok kontroll?

En utfordring som mange organisasjoner har som sitter på mye informasjon om mange er hvordan man skal sikre seg mot uautorisert bruk, gjerne fra egne ansatte. Utfordringene er også knyttet til feilaktig registrering og feilaktige treff, og de faktiske følgene det vil få for enkeltpersoner. Min informant i Datatilsynet understreker:

> *«Det ligger i sakens natur; ja, det er veldig inngripende for den det gjelder og det har blitt vurdert som nødvendig og derfor har man også supplert med å ha en veldig detaljert særordning på området. Dette har gitt Datatilsynet konkrete oppgaver knyttet til det, selv om det var middels godt ivaretatt når vi gjorde kontroll på det, og vi har internasjonal oppfølging på området. Når en har sett det nødvendig å etablere dette i Schengen så har en supplert også*

med tiltak som skal balansere det, så det er et område som blir fulgt tross alt relativt godt opp. Også sett i lys når vi ser mot 2013 hvor vi har på plass en god regulering av behandlingen av personvern i politiet for øvrig så fins det jo balanser der».

Når det gjelder SIS II hadde ikke Datatilsynet i forkant startet arbeidet med å sette seg inn i det nye systemet ennå, det er noe de vil gjøre når de trenger å være på banen. Det er diskusjoner internasjonalt knyttet til dette der Datatilsynet sitter i personverngruppen. Men det ville vært fordelaktig om Datatilsynet var mer deltakende i prosessen allerede fra starten av. Da ville Datatilsynet hatt mulighet til å komme med innspill før veien var helt staket ut for SIS II. Kommer man inn i ettertid kan endring være vanskelig å få til, og man vil på mange måter gjenta historien fra Norges første møte med SIS. Det er sannsynlig at dette også dreier seg om et spørsmål om kapasitet i Datatilsynets daglige virke, dessuten kan det nok kreve en del å skulle følge tett med på utviklingen av et nytt system som blir til utenfor Norges grenser. Man vil også måtte samarbeide i større grad med tilsynene i de andre land.

Min informant mener at kontrollen på dette området er stor sammenliknet med andre områder. Når det gjelder Kripos sin kontroll internt var det funn knyttet til dette i tilsynet som tydet på at noe kunne bli bedre. Men her er det gjort tiltak og politiet er i følge min informant i en god modningsprosess nå. I ettertid har Kripos igjen blitt fulgt opp og det er blitt gjort både tekniske og administrative korreksjoner. Det har også blitt gjort rolleavklaringer mellom Kripos, UDI, og Politiets Data- og Materielltjeneste som vil drifte informasjonssystemene.

Min informant nevner at Politiregisterloven som er på trappene og som venter på ikrafttredelse vil gjøre at Datatilsynet vil få et tilsvarende mandat overfor politiet generelt. Slik er det ikke i dag. Denne vil mest sannsynlig tre i kraft i løpet av 2013.

Et av ankepunktene med hensyn til spesielt SIS er antakelsen om at det har vært og er ulik praksis landene i mellom – man er redd for at dette kan ha en negativ innvirkning på personers rettssikkerhet. En av mine informanter meddeler at det finnes en form for datatilsyn i hvert medlemsland, noe som er et vilkår for å bli medlem av Schengen og Europarådet, men stiller seg likevel tvilende til om det har noen effekt i dette internasjonale systemet.

«Det er ulike tradisjoner, det er ulike oppfatninger, det er ulike definisjoner av ting som er gjenstand for praktisering innenfor Schengenavtalen, så det at man skaffer seg et datatilsyn, det betyr ikke så veldig mye».

Min informant påpeker at det er avgjørende med et internasjonalt samarbeid også mellom tilsynsmyndighetene. Det at vi har et administrert regelverk gjør at tilsynsmyndighetene i de

ulike landene har felles organ og likt regelverk å forholde seg til. Styrken her ligger i at man har mulighet for å søke råd og be om bistand fra samarbeidende myndigheter. Det understrekes overfor meg at Datatilsynet ser på en forordning på personopplysningssiden – det er et utkast ute til en ny forordning som vil tre i kraft i norsk rett de nærmeste årene. Dette vil føre til en ytterligere modernisering, og et felles harmonisert regelverk på personvernopplysningsområdet er viktig. Dette har blitt trykket på gjennom vårt «støttemedlemskap» i EU.

En av mine informanter påpeker at det som finnes i systemene er esoterisk informasjon, den er vanskelig tilgjengelig og *kun tilgjengelig for noen ytterst få*. Mengden av systemer og deres tekniske og komplekse natur gjør at han reiser spørsmål ved hvordan man i det hele tatt skal kunne føre kontroll med disse. Han betviler også at de som sitter på Stortinget har noen som helst kunnskap om Schengen og hva dette egentlig innebærer.

En av informantene mener vi vil få en verbal oppslutning rundt personvern og at vi vil få hjemler til å gjøre personvern gjeldende. Det som kan komme til å bli et stort problem er å øve kontrollvirksomhet og tilsynsvirksomhet på dette området, for det blir så mye å holde øye på. Det blir rett og slett et kapasitetsproblem. Det er ikke så mange norske forvaltere av personopplysninger som har fått tilsyn i løpet av de siste 20 årene.

> *«det er elementer av skjønn og vi vet jo stadig klarere at alle slike kontrollmekanismer hvor det kommer inn momenter av skjønn blir vanskelig å håndheve på en måte som folk oppfatter som saklige og rettferdige. Regelverket er det ikke noe galt med, men det er skjønnselementer som da tolkes forskjellig, og da får man ulikhet».*

Mathiesen (2013) påpeker at det er ikke gitt at vi selv med presise reglement knyttet til systemene klarer å henge med i den farten systemene og teknologien utvikler seg.

Det ser ut til at det selv med regler har oppstått en gråsone der det fremdeles er noe uavklart hva som er oppgavene og myndigheten til de nasjonale domstolene og de nasjonale datatilsynene knyttet til vern av personers data og rettigheter (Brouwer, 2008). EDPS og JSA er også utøvere i det totale kontrollbildet, men det ser ikke ut til å være stor grad av samarbeid mellom disse. Dette kan føre til at SIS faller mellom flere stoler. Når man i tillegg utveksler informasjon mellom ulike system og over grensene vil kontrollblikket til landenes egne tilsyn falle av på veien. Man har altså en kontroll, men den ser ikke ut til å være tilstrekkelig. Slik sett blir størsteparten av og den viktigste delen av kontrollfunksjonen overlatt til utøverne av

systemet selv. De som legger inn opplysninger, tar ut opplysninger og anvender disse i sitt daglige virke.

5.7 Non-Governmental Organizations (NGO)

I mitt arbeid har jeg kommet over og i kontakt med organisasjoner og foreninger som engasjerer seg i personverndebatten. Det som kjennetegner disse organisasjonene er at de i utgangspunktet er non-profit og ikke har annet brensel enn sitt eget og forhåpentligvis andres engasjement. Flere av disse har satt lupen på personvern i Schengen-samarbeidet.

Disse organisasjonene kan ses på som en motvekt til statlige organisasjoner, og er en viktig kritisk motrøst. Her følger en fremstilling av «NGO» som begrep og det vil bli diskutert rundt deres ståsted og nytteverdi. Jeg vil gi en fremstilling av NGO's jeg har kommet i kontakt med og hvordan disse bidrar i debatten med deres synspunkter.

5.7.1 Hva er en NGO?

Non-governmental organizations (NGO), eller ikke-statlige organisasjoner, er et forholdsvis moderne fenomen, og de blir gjerne til med en målsetning om å fremme interesser og stå opp for siviles rettigheter og behov (Paul, 2000). Det er store forskjeller organisasjonene i mellom hvordan de arbeider; noen vil stå på barrikadene og demonstrere, mens andre er opptatt av å spre informasjon og sitt ideologiske budskap ved langt mer rolige fremgangsmåter. En del NGO's tenderer også til å bygge nettverk og gruppere seg med andre organisasjoner med sammenfallende interesser som kan bidra til å gjøre dem mer slagkraftige. Denne typen organisasjoner har også en tendens til å vekke stor tiltro blant folk, og det hender at tilliten faktisk er større til de ikke-statlige organisasjonene enn til statlig funderte virksomheter (Paul, 2000).

En NGO vil skille seg fra den beslektede grasrot-organisasjonen ved at grasrotorganisasjonene som regel er medlems-basert, og dette er ikke nødvendigvis tilfellet for en NGO (Holmén og Jirström, 2009). Grasrotorganisasjonene har som oftest også en mer lokal forankring og interessefelt. NGO's er som oftest å finne i urbane områder og er gjerne drevet av profesjonelle eller semi-profesjonelle tilsatte (Holmén og Jirström, 2009).

Grasrotorganisasjonene blir ofte sett på som små og svake med lite slagkraft – dette er ikke nødvendigvis tilfellet for en NGO.

En NGO kjennetegnes gjerne av å være non-profit (Paul, 2000). Dette medfører riktighet til dels. En NGO er ikke «forretningsdrevet» slik en vanlig bedrift vil være, men drevet av interesse og engasjement knyttet til et saksområde. For å kunne sikre sin overlevelse er disse organisasjonene likevel ofte avhengige av donasjoner, salg av bulletins, små reklameprodukter osv. Det er en tendens til at mange NGO's går i en mer kommersiell retning i større grad enn vi har sett tidligere, og der den kommersielle delen ser ut til å være i ferd med å overta for det den startet som. Det er således også viktig å være klar over de farer som er forbundet med å motta store pengebeløp fra enkeltpersoner eller bedrifter; dette kan lede til forpliktelser selv om man i utgangspunktet hadde mål om å tjene en større krets (Paul, 2000).

Det er en tiltagende tendens at disse organisasjonene sprer seg internasjonalt (Paul, 2000). Dette forklares som en effekt av globalisering, samtidig som «mannen i gaten» har et økende behov for å holde kontroll med hva statlige virksomheter egentlig holder på med.

Denne typen organisasjoner omtales ofte som «watchdogs» da de ofte har et overvåkende og kritisk blikk på det de statlige virksomheter foretar seg (Holmén og Jirström, 2009). Det er også vanlig at de kjemper for den «svake» part i en sak.

Ofte argumenterer man for at man bør gi disse organisasjonene en mer formell stemme i EU (Holmén og Jirström, 2009). Det er flere medlemsland som ikke nødvendigvis fronter deres borgeres interesser. Har man en NGO med på laget har man en aktør som kan påse at deres interesser ivaretas.

En innvending til dette er at selv om disse organisasjonene tilsynelatende vil kjempe for folks rettigheter, så er det ikke alltid de er i så stor grad demokratiske og gjennomsiktige (Holmén og Jirström, 2009). Det er en mulighet for at de ikke tjener alles interesser, men heller visse sosiale lag. Dette kan også knyttes opp mot støtte og donasjoner som nevnt tidligere. Det vil også være slik at de mest organiserte gruppene vil komme mer frem i lyset i motsetning til de som holder seg mer i bakgrunnen (Holmén og Jirström, 2009).

Det finnes organisasjoner som har klart å komme seg på innsiden i EU, og som har blitt en stemme man tar med i betraktningen i ulike saker (Holmén og Jirström, 2009). Deres mening

blir ofte ansett som verdifull, gjerne på bakgrunn av at de sitter på en spesiell kompetanse på sitt felt, selv om de ikke er i besittelse av en formalisert makt slik som de statlige aktørene.

Det er nærliggende å anta at for å klare dette kan man ikke være den største kritikeren eller representere den største «faren» (Holmén og Jirström, 2009). På bakgrunn av dette er det legitimt å reise spørsmålet om en slik deltakelse vil ha noen verdi og representere en *alternativ* stemme. Som det påpekes av Loader og Walker (2007) kan heller ikke en slik organisasjon komme med en kritisk pekepinn foruten å ha et konstruktivt tiltak. Man kan heller ikke fronte utopiske tanker som ikke kan oppnås (Loader og Walker, 2007). En NGO vil i dette henseendet måtte vokte seg for å bli «sugd opp» i en annen organisasjon og således miste sin kraft som uavhengig aktør.

Det er også kanskje å ta noe i å konkludere med at en NGO vil representere det sivile samfunnet som helhet, men representerer gjerne heller en gruppe med sine interesser og agendaer. Et problem som kan reise seg i dette henseendet er at publikummet blir for smalt slik at man ikke når frem til allmennheten.

5.8 Statewatch

Statewatch sitt arbeid oppsummerer seg godt i en setning på deres hjemmesider: «*monitoring the state and civil liberties in Europe*» (Statewatch.org, 2013b 10.2.2013). Statewatch som organisasjon ble opprettet i 1991 i London, selv om arbeidet ble startet lenge før dette. Organisasjonen består av journalister, akademikere og forskere og har bidragsytere i 18 land. Statewatch samarbeider også med andre grupper og organisasjoner. Deres arbeid er i utgangspunktet non-profit, selv om de gir ut og selger bulletins samt mottar støtte som jeg vil vise senere. Via deres nettsted og publikasjoner setter Statewatch søkelyset på saker som ellers får liten eller feil oppmerksomhet i media. Statewatch setter i stor grad hele EU under lupen og er en viktig stemme for å sette pekepinn på eventuelle utfordringer og problemer og er en av de mest sentrale informasjonskildene på området. Statewatch er i følge deres nettsted det mest omfattende stedet på internett for analyser rundt EU og innenrikspolitikk, med en database med over 29000 artikler i skrivende stund (Statewatch.org, 2013b 10.2.2013). Statewatch har ikke latt Schengen-samarbeidet gå ubemerket hen, og det var viktig for meg å oppnå kontakt med representanter for organisasjonen.

5.8.1 På pub med Statewatch

Mitt møte med Statewatch fortjener et eget avsnitt. På egen hånd kontaktet jeg organisasjonens leder Tony Bunyan ved flere anledninger per mail uten å lykkes. Jeg fikk til slutt kontakt og fikk en intervjuavtale ved hjelp av Thomas Mathiesen som kjenner Bunyan og tidligere også har besøkt organisasjonen. Selv om vi inngikk en intervjuavtale fikk jeg dårlige nyheter et par uker før avreise til London. Årsmøtet til Statewatch hadde blitt besluttet lagt til selve intervjudagen, og deres tid var knapp. Vi fikk heldigvis avtalt et møte etter deres arbeidstid, og vi møttes på en pub sentralt i London. Jeg ble møtt av organisasjonens leder og redaktør Tony Bunyan og en av hans medarbeidere Chris Jones. Bunyans utømmelige kunnskapsbrønn som har blitt til gjennom et iherdig engasjement over flere tiår i kombinasjon med den unge entusiastiske og velinformerte Jones gjorde dette møtet til en svært positiv og lærerik opplevelse jeg ikke ville vært foruten.

Det er litt ukonvensjonelt å gjennomføre et intervju av denne sorten på en pub, men det eneste problemet jeg merket meg under intervjuet var støynivået. Elles hjalp dette uhøytidelige miljøet oss til raskt å få kontakt på et nesten «kameratslig» plan, og praten satt løst, slik at jeg kan ikke si at miljøet dette intervjuet ble foretatt i var ødeleggende for intervjuets kvalitet. Det var heller ikke temaer som skulle diskuteres som var av lyssky karakter. Det som riktignok gjorde dette til det mest anstrengende intervjuet i rekken var en kombinasjon av støy og at intervjuet ble fortatt på engelsk av to svært snakkesalige engelskmenn. Båndopptaker ble heldigvis benyttet.

5.8.2 Statewatch som informasjonsformidler

Statewatch startet med 2 ansatte på kontoret i London og 2 arbeidere utenfor UK. Organisasjonen har nå ekspandert til et nettverk bestående av 34 tilknyttede personer i 18 land og samarbeider også med andre organisasjoner. Samarbeidspartnernes bidrag er sporadiske og ikke kontraktsfestet. Mine informanter forteller meg at folk gjerne tror de er større enn de egentlig er og svært mange har hørt om dem. Koker man arbeidstimene ned er de ikke større enn om lag 5 årsverk. Det gir et godt bilde på at Statewatch har klart å skape seg en plass og fått publisitet, selv om organisasjonen i utgangspunktet er nokså liten.

Før internett ble en av de viktigste kanaler for informasjonsspredning publiserte Statewatch en bulletin 6 ganger i året og var deres viktigste kommunikasjonsmiddel. Denne gikk ut til abonnenter og ble nøysommelig pakket og sendt fra deres kontor til deres abonnenter. Lesertallene har sunket noe, men har til gjengjeldt økt betraktelig elektronisk. Internett har gjort spredningen av informasjon mye enklere og raskere og bidrar til å nå ut til et bredere publikum. Statewatch har i løpet av en måned rundt 100.000 besøkende på sine nettsider (Statewatch.org, 2013b 10.2.2013).

Organisasjonens leder, Tony Bunyan, drev i sine yngre dager utstrakt reisevirksomhet til Brussel og Luxembourg og fulgte det politiske liv «hands-on». Disse besøkene var viktige i deres nettverksbygging der journalister ville høre deres meninger og verdifulle kontakter ble skapt. Dette gav også Statewatch mulighet til å fronte deres meninger og de fikk også tilgang til uoffisielle kilder for informasjon. I ettertid har Statewatch i tillegg knyttet til seg personer som behersker ulike språk som fransk, slik at originaldokumenter kan oversettes. På spørsmål om hvor de får tak i informasjon får jeg humoristisk til svar: «*Jeg er journalist. Det vil jeg aldri avsløre»*.

Mine informanter forteller at deres hovedfelt er sivile rettigheter, frihet og menneskerettigheter. Statewatch står ikke på barrikadene, men gir de på barrikadene *ammunisjon* til å forstå hva problemene er og hva det egentlig er de er i mot. Statewatch selv driver ikke med kampanjer, men fôrer andre med info slik at de kan drive sitt arbeid på et bedre grunnlag.

Det understrekes overfor meg at folks meninger svært ofte er basert på feil eller halvsannheter. Statewatch er ikke interessert i å bidra med drivstoff slik at de tabloide mediene kan skrive store oppslag om «de hundretusener av immigranter som er på vei inn i landet for å ødelegge livene våre», selv om dette sikkert kunne bidratt til å gi Statewatch enda større grad av publisitet. Målet er å få ting frem i lyset til et større publikum, men under riktige forutsetninger. Et viktig mål for Statewatch er derfor å gi folk informasjon slik at man kan debattere temaer på en mer riktig måte. Det understrekes overfor meg at i et demokrati bør man ha *informert enighet* og *informert uenighet* – disse er likeverdige.

5.8.3 Er Statewatch en NGO?

På mitt spørsmål om Statewatch er en NGO får jeg inntrykk av at dette dreier seg om et definisjonsspørsmål. Det som gjerne kjennetegner en NGO er at de er helt løsrevet fra stat. I Statewatch sitt tilfelle er dette noe mer komplekst.

Til min overraskelse kommer det frem under intervjuet at Statewatch de siste 3-4 årene har mottatt støtte fra Europakommisjonen. Statewatch skriver et program som Europakommisjonen godkjenner. Jeg reiser spørsmålet om dette legger føringer og virker manipulerende på deres arbeid. Dette forkastes av mine to intervjuobjekter. Da Statewatch selv skriver programmet mener de selv at de på denne måten ikke danser etter EU's pipe. De bidrar med et viktig og nyttig arbeid også overfor EU, ved at de undersøker, samler inn og gjør mengder av informasjon tilgjengelig for allmennheten. Spesielt ved deres evne til å koke ting ned slik at komplekse ting blir mer lettfattelig. De fungerer også som forskere og sitter på en stor database av informasjon som allmennheten kan søke i. De arbeidet i over 15 år uten støtte annet enn en beskjeden inntekt på deres bulletins, så kursen var vel på en måte allerede satt. De er åpne om støtten og setter sin egen agenda slik de alltid har gjort. Deres arbeid er viktig fordi de ofte adresserer problemer der søkelyset ikke har vært rettet. Jeg sitter med inntrykk av at de har tatt jobben med å være en kritiker og på denne måten gjør EU en tjeneste, samtidig som de er en viktig bidragsyter.

I følge leder Bunyan kan Statewatch sees på som en NGO dersom man ser stort på det, men kan også falle inn under kategorien «think tank».[6] Organisasjonen er registrert som en «*research and education trust*». De er begge enige i at Statewatch er en sammenblanding av flere kategorier, og det kan være dette som gjør dem noe unike.

5.8.4 Schengensamarbeidet – en del av et system i ulikevekt

Mine informanter gjør det raskt klart at definisjonen av terrorisme kom feilslått ut etter terrorangrepet i New York i 2001, og dette fikk katastrofale følger for demokratiet og den menneskelige frihet. Bunyan fremstiller dette som en vektskål med krav om sikkerhet på den

[6] «Think tank» kan defineres som en organisasjon eller gruppe som utfører arbeid og forskning knyttet til eksempelvis politiske tema. Arbeidet er for det meste non-profit og ideologisk drevet (sourcewatch.org).

ene siden og privatlivet på den andre. Det gis uttrykk for at terroren i New York kan ha bidratt som en unnskyldning eller legitimering til større grad av overvåking og tillagt privatlivet mindre vekt, også i Europa.

Schengen har skapt det mine informanter omtaler som en «continental entry ban» fra inntrengere utenfor Europa. De som befinner seg på innsiden skal kunne bevege seg fritt, men dette vil ikke gjelde alle. Hvordan skal man eksempelvis vite om en person med afrikansk utseende har bodd her i 20 år, eller har kommet seg ulovlig inn? Mine informanter påpeker at mange blir stoppet og sjekket gjentatte ganger på gaten uten å ha gjort noe som helst. Dette fører til at en på bakgrunn av ens utseende konstant vil befinne seg i «mistenkt»-kategorien. Retten man har til å bevege seg fritt rundt i Europa gjør samtidig at myndighetene kan tillate seg større kontroll av oss. Denne retten vil således være noe innskrenket for dem som til stadighet faller inn under politiets «kontrollupe».

Spørsmålet reises også av Statewatch om hvor verdifull informasjonen egentlig er. Systemene blir større og mer komplekse, et godt eksempel på dette er SIS II. I likhet med Sheptycki (2007) som vist tidligere reiser mine informanter i Statewatch spørsmålet om det er en mulighet at man ikke vil få benyttet all informasjonen man lagrer. Det legges til at det virker som det er en forvirring mellom Europol og de andre systemene. Mine informanter mener de begynner å overlappe. Det er heller ikke så mange treff man får i databasene. I tillegg kan dette ha såpass store konsekvenser for individers rettssikkerhet og privatliv. De reiser spørsmålet om alt dette «styret» er verdt det for at man skal slippe å vise passet når man skal ta seg en tur til Frankrike.

Det vil alltid være en viss fare med at systemer, også SIS, blir misbrukt på en eller annen måte. Bunyan nevner hendelsen for noen år tilbake der en belgisk politimann ble tatt for å ta ut informasjon og selge denne videre til organiserte kriminelle.

Uansett hva man vedtar av lover og regler vil man være helt avhengig av at landene følger reglene og at de som er satt til å jobbe med det faktisk gjør det de er satt til å gjøre.
På spørsmålet om det er forskjeller i praksis svarer mine informanter bekreftende på dette, fordi man uansett vil følge nasjonale lover, som det også oppfordres til i Schengenkonvensjonen. Praksis med hensyn til hvilke kriterier informasjon legges inn etter vil også variere. Faren for at andre land kan *legge til* informasjon på en eksempelvis ettersøkt eller uønsket for så å levere denne videre til et annet land igjen vil føre til at man har svært

liten kontroll med hva som foregår. Det understrekes overfor meg at vi bare ser toppen av isfjellet når det gjelder saker der folk blir lagt inn i SIS på feilaktig eller ulikt grunnlag, det vil være mange situasjoner vi ikke kjenner til og aldri vil få kjennskap til.

Et annet problem som kun blir nevnt av mine informanter i Statewatch er at informasjonssystemene som benyttes i EU vil strekke over land med ulike språk, og dermed også ulike alfabeter. Dette kan føre til stavefeil som kan få store konsekvenser. Dersom man eksempelvis skal føre en person fra et land som Kina inn i systemet må navnet «oversettes» til latinske bokstaver. Når disse flyttes fra system til system vil dette kunne danne følgefeil og nye feil kommer til i forskjellige skjemaer og databaser. Man har skaffet systemer som skal bidra til å gjøre dette som feilkilde minimal, men om dette systemet er «vanntett» kan man selvsagt stille spørsmål ved. Det er grunn til å tro at ved manuell føring av informasjon vil det enkelt kunne oppstå små feil i passnummer, bilregistreringsnummer og liknende. Man kan jo bare tenke seg hva slags fatale konsekvenser det kan få om man får ført sitt passnummer inn i et system av denne sorten ved en feiltakelse, eller plutselig overtar et bruddstykke av en annen persons identitet.

Som diskutert tidligere har man krav på innsyn og å få rettet eventuelle feil, i hvert fall på «papiret» med sine mange unntak. I følge Statewatch er det avgjørende at vi får innsyn og at dette går begge veier. Men det er i stor grad et system preget av enveistrafikk.

Noen land ligger også langt etter med tanke på hvordan informasjon lagres. Det finnes land som fremdeles opererer for det meste med papirjournaler. Man kan lett forestille seg hvilken enkel operasjon det vil være å ta ut et par dokumenter, kopiere dem, for så å sette disse tilbake.

England er ikke medlem av Schengen og dette forklarer Statewatch ved at England er svært opptatt av å selv holde kontroll med hvem som forflytter seg over deres landegrenser, og det legges til at de også later som at de har kontroll. Etter opplysninger fra Statewatch fikk England *tilgang til SIS i 2003*. Kripos på sin side avkrefter dette. Dersom et land får tilgang til SIS uten å være medlem av Schengen kan det sees på som en måte å skumme fløten der de har tilgang til informasjon, men slipper medaljens bakside; fri gjennomstrømning inn til landet. Dette kan settes i sammenheng med Kvams (2008) betegnelse «cherry picking». Kunne dette vært et alternativ for Norge?

Mine informanter nevner at mange i EU mener at man kan få orden på noe som egentlig er et sosialt problem ved bruk av teknologi. Når folk krysser havene for å komme seg inn til Europa er det ikke nødvendigvis en god løsning å sende ut et Frontex-helikopter, men man bør heller se på hva som er årsaken til at disse menneskene ønsker å forlate sitt hjemland i utgangspunktet. Denne delen som åpner opp for en helt ny problematikk ser ut til å være helt glemt.

5.9 International Commission of Jurists (ICJ)

International Commission of jurists (ICJ) er en NGO som har til formål å vokte over rettsstaten og påse at menneskerettighetene blir ivaretatt. Dette er rent basert på frivillig arbeid. To av mine informanter er deltakende i den norske avdelingen; daglig leder Jon Wessel-Aas og Ketil Lund. De fleste EU-land har en gruppe. Det er imidlertid noe variert hvor aktive gruppene er – noen har avdelinger som ligger døde eller sovende.

ICJ ble stiftet i Geneve og opprettet etter andre verdenskrig i samme ånd og i klar sammenheng med opprettelsen av FN's menneskerettighetskonvensjoner, Europarådet og den Europeiske menneskerettighetskonvensjonen av jurister.

Min informant forteller at dommere, akademikere, jurister og advokater så et behov for en organisasjon av *uavhengige* jurister fra forskjellige sektorer. Man hadde sett grusomme overgrep på alminnelig menneskerettigheter, man hadde sett hvordan domstoler opptrådte og hvordan noen gikk i nazismens tjeneste.
Man har nasjonale avdelinger i ulike land, og man utretter samme type arbeid fra et nasjonalt perspektiv som det internasjonale kontoret med fast sekretariat og med fast ansatte jurister gjør fra Geneve. Organisasjonen er fast høringsinstans både i FN og i Europarådet på internasjonalt nivå. Dette tyder på at organisasjonen er høyt ansett og man er villig til å ta deres bidrag i betraktning.

> *«(…)blander seg inn, ja det gjør de for så vidt med meninger. Det varierer litt fra land til land hvordan man er organisert der. De ressursene man har… I England for eksempel som er et mye større land der er ICJ integrert i en organisasjon som heter Justice… som er en stående organisasjon med faste ansatte, ansatte jurister, som i motsetning til hva vi kan gjøre her i Norge… de har ressurser til å påta seg saker og føre saker i domstolene for parter som ellers ikke ville hatt råd til det eller tatt seg råd til det for å få prøvd prinsipielle spørsmål. Litt sånn*

> *som man kjenner fra USA, der har du jo ACLU (American civil liberties union), som er en stor organisasjon med mange faste ansatte advokater».*

Norsk avdeling har et styre og et fagutvalg på forskjellige sektorer, totalt rundt 30 aktive medlemmer. Disse jobber i fagutvalgene og forbereder høringsuttalelsene. Dette er «dugnadsarbeid» og alle har annet arbeid til daglig. Arbeidet har ofte et «ad-hoc» preg, og det kan dukke opp ting der man må mene noe.

> *«Vi har bare medlemskontingenter og det er rent gratisarbeid vi driver med (…) vi er mer sånn at vi skriver høringsuttalelser på lovgivning som berører disse spørsmålene, eller arrangerer seminarer, debatter, skriver aviskronikker, blander oss på den måten. Ad-hoc basert; «her må vi mene noe!»*

Min informant understreker at de ønsker å peke på ting de mener svikter i forhold til det han kaller «menneskerettighets-instrumentene» som eksisterer, altså konvensjoner på et rettslig plan. Man vil peke på ting når man ser at en beveger seg ut i en gråsone som bør utredes bedre, eller når man ser at myndighetene har oversett eller gått for langt. ICJ er også opptatt av å overvåke lover som presser seg på utenifra.

> *«(…)det er ikke noe mer aktivistisk enn det. Det kan virke sånn, for det er mange myndigheter som bevisst eller ubevisst gir ganske blaffen, så det kan høres ut som man er politisk aktivist som vil at ting skal være annerledes enn det er, men meningen er at når vi lager litt bråk så er det ikke annet enn at nå er det ikke opp til standard, altså det går rett og slett ikke an å gjøre sånn».*

Det som er knyttet til personvern og innsamling av informasjon fra politimyndighetene i Norge er noe ICJ kommer i kontakt med mer indirekte. ICJ vil ofte peke på at man ikke bare må se på vilkårene for å samle inn informasjon her og hva det skal brukes til, men i hvilken grad informasjonen flyter ut til samarbeidende tjenester, hvordan det foregår og hvilken kontroll det er med det.

Min informant påpeker at utviklingen har gått svært raskt, og sivile organisasjoner som har meninger om ulike ting har vanskeligheter med å bli hørt. Man skal likevel ikke undergrave viktigheten av disse organisasjonene som kan minne oss på og påpeke farer vi ellers ville ignorert eller ikke vært klar over. Media har et stort ansvar for å bidra i kraft av sin evne til å nå ut til mange, noe som vil være en stor utfordring for en non-profit organisasjon med få ressurser tilgjengelig.

Jeg kan ikke konkludere med at de ikke-statlige organisasjonene har en kraftfull effekt. Til det er de små og i mindretall som nok fører til at de «drukner» i møtet med det de ofte forsøker å

utfordre. Deres arbeid er likevel ikke forgjeves. De bidrar langt på vei til å sette viktige saker på dagsorden som ellers for de fleste ville gått helt eller delvis ubemerket hen. Så vil det i større grad være opp til media og enkeltindivider å spre deres budskap. Det er liten tvil om at de burde gis bedre plass i formelle sammenhenger. Også de som ikke er så høyt ansett som ICJ, som nok automatisk vil få en høy status da organisasjonen utelukkende består av jurister.

Det kan nevnes at tidlig i prosessen var det ønskelig fra min side å gjennomføre intervju med Nicholas Busch, redaktør av «Fortress Europe», men jeg ble gjort kjent med hans bortgang. «Fortress Europe» var et såkalt ”circular letter”, og senere en blogg med samme navn som så på Schengen-samarbeidet med et kritisk blikk. Nicholas Busch og hans arbeid fungerte som en viktig bidragsyter og «overvåker» av Schengenmaskineriet.

5.10 Sivilblikket som kontrollfaktor

Det at «vanlige» mennesker er informert og holder et øye med beslutninger som blir tatt av de offentlige myndigheter kan være et viktig kontrollaspekt i seg selv. Når man har egne instanser som har som sitt virke å drive kontroll kan kanskje et slikt aspekt falle litt i bakgrunn.

Det de fleste av oss vet om politiarbeid er filtrert gjennom mediekonstruksjoner (Bowling og Sheptycki, 2012). Deler av politiarbeidet er i stor grad hemmeligholdt, dette gjelder spesielt det internasjonale arbeidet. Arbeidets natur vil også naturlig nok kreve en viss grad av hemmelighold dersom det skal være nyttig. I følge forfatterne av ”Global Policing” bør nettopp dette temaet være noe av det viktigste å være opptatt av i vår tid. Dårlig politiarbeid skaper usikkerhet (Bowling og Sheptycki, 2012). Siden politiarbeid er nokså skjult ekspanderer systemet ”bak ryggen” vår nesten uten at vi merker det. SIS bærer karakteristikk av å være et veldig lukket system og kritikerne påpeker at det har blitt til på en svært udemokratisk måte, noe som politiet har bidratt til. Kun et fåtall av personer fra ulike nasjoner har bidratt til utformingen av systemet. Systemet ser ut til ikke å inngå i særlig grad i den offentlige debatten og folk flest kjenner i liten grad til dette (Bowling og Sheptycki, 2012). Dermed faller kontrollaspektet som allmennheten burde bidra med noe vekk.

5.10.1 Brød og cirkus – befolkningens og medias manglende interesse

En viktig «kontrollør» vil være den generelle befolknings røst. Men når det gjelder informasjonssamarbeidet i Schengen synes denne å være svak. I likhet med Thomas Mathiesen (2000) undrer jeg på hvorfor Schengen og dette temaet ikke har vært oppe til debatt i særlig utstrekning de siste årene før inntil nylig.

«Offentlighet er og blir den beste kontrollmekanismen. Avsløring av kritikkverdige forhold vil ofte, gjennom media, bli gjort offentlig for en større krets. Dette er også viktig for samfunnsdebatten». (Ny offentlighetslov, 2003:30).

Dersom folk blir informert om det som foregår vil dette kunne bidra til å heve kvaliteten på offentlige beslutninger (Loader, 2002). Skal offentligheten ha mulighet til å vise interesse og ha noen som helst mulighet for å følge med krever dette at media er på banen. Media har ikke gjort plikten sin med å opplyse folket om dette, og den politiske interessen har vært minimal (Bowling og Sheptycki, 2012). I følge Bowling og Sheptycki (2012) ser det ikke lyst ut for fremtiden, og det dras til og med paralleller til Europas fortid. Offentlighetsprinsippet vil gi enhver mulighet til å utøve en viss form for kontroll overfor forvaltningen (Eskeland, 1988). Men dersom media ikke er interessert i dette skal det godt gjøres at dette når frem til publikum.

Flere av mine informanter meddeler at norske journalister blir veldig fort trette. De få gangene noen har forsøkt å ta opp dette har det ikke blitt noe oppslag i media i det hele tatt. Det skjer så mye nytt som er mer spennende. «*Den relasjonelle kondisjonsevne er ikke spesielt imponerende»*. SIS og Schengen er relativt tung materie og det er kanskje ikke det som bidrar mest til å selge aviser.

Jeg stiller meg undrende til hvorfor eksempelvis Datalagringsdirektivet, som kanskje det eneste, har fått så stor mediedekning og har fått sinnene i kok hos den vanlige borger, mens Schengen og spesielt overvåkingen forblir nesten ukjent. En av informantene mener dette ikke angår oss på samme måte, og det er lettere å forstå for en vanlig borger for eksempel at ens mobiltelefon og mobilbruk kan komme til å bety noe. Det har nok noe å gjøre med avstanden til problemet – det er lettere å kunne sette seg inn i og interessere seg for noe som kan angå en på denne måten enn personer som kommer over grensene fra tredjeland, inntil disse menneskene blir synlige for oss som nå er situasjonen i norske byer. Det blir mer konkret. Det

understøttes også av andre av mine informanter at det hele tiden veksler hva som er oppe i folks bevissthet, alt fra terror til internasjonale pedofilinettverk til internasjonale ransbølger. Media har en viktig rolle i styringen av dette. Apenes støtter opp under dette og understreker at en avvikling av privatsfæren er mindre håndgripelig enn andre ting som opptar oss som krig og sultkatastrofer (Apenes, 2000). En av mine informanter føyer til:

> *«Folk flest er opptatt av brød og cirkus. Og media og politikere og befolkningen de inngår jo i et slags symbiotisk forhold… hvor mennesker er irrasjonelt redde til en hver tid for kriminalitet, og denne redselen den virker i en slags vekselvirkning. Media da som først og fremst driver den frem gjennom sine spektakulære reportasjer og politikere som bruker denne redselen som et grunnlag for mer populistiske holdninger og angstdempende forslag om alle mulige slags tiltak. Og når jeg sier at folk flest bare er opptatt av brød og sirkus, så er det da fordi de er grunnleggende utrygge og redde, og så lenge den redselen da kan bli beroliget så er vi egentlig ikke opptatt av noe som helst annet enn å bli underholdt. Og få nok å spise og ha det koselig».*

Det er nærliggende å anta at så lenge redselen og utryggheten opprettholdes kan den benyttes til å legitimere de fleste overvåkings- og kontrolltiltak så lenge det kan ha en beroligende effekt. Dette er sammenfallende med det dilemmaet Burke (2002) påpeker: "*security is bound into a dependent relation with «insecurity», it can never escape it: it must continue to produce images of "insecurity" in order to retain its meaning"* (Burke i Fierke, 2002). Kan det på bakgrunn av dette være riktig å påstå at vi trenger usikkerheten for å kunne ha en formening om sikkerhet?

> *«(…) om det er overfallsvoldtekter, eller om det er terror, det selger på en måte, men altså det passer så godt, det er så utrolig kjedelig å skrive om sånn som vi snakker om nå om lovarbeid og hvordan det bør settes sammen ikke sant, det er ikke noe sexy i det hele tatt. Men at de jobber i en selvforsterkende syklus, sikkerhetsindustrien eller sektoren som bare ser farer, altså for det er jobben deres (…) det er bare en haug med potensielle kriminelle der ute, og vi vet søren ikke hvem det er som er den neste, og det preger måten de tenker på, og så selger media på en veldig overdimensjonert måte hvor farlig alt rundt oss er. Og så ber de samme tjenestene om at hvis vi skal gjøre dere trygge, så må vi ha dette, for politikere så er det veldig vanskelig å si nei, når det først har kommet ut, og for det andre så er det utrolig billig.»*

Min informant legger til at det er en helt vanlig oppfatning at "jeg har jo ikke gjort noe galt", så da gjør det jo ikke noe at det registreres alt det en driver med. Dette er en vanlig oppfatning som igjen baserer seg på tillit som også gjør at denne gjennomsiktigheten godtas. Men samtidig er den basert på en irrasjonell tillit til at opplysninger aldri vil bli misbrukt. Som en av informantene fra Statewatch humoristisk sa men med en seriøs undertone: «*Nothing to hide, nothing to fear. If you have nothing to hide you must have lived a very boring life".* Det

han nok prøver å formidle med denne noe humoristiske uttalelsen er at selv mennesker med «rent mel i posen» har personopplysninger som alltid vil ha en verdi. Man er derfor avhengig av et engasjement fra folket, for dette er noe som angår alle.

> *«Problemet med dette er at det man skal regulere her er stort sett en måte å kontrollere «de andre» på. De kriminelle er heldigvis et mindretall i ethvert samfunn, og i stor grad når det gjelder hva vi snakker om nå, terror eller Schengen, så er det i enda større grad i andre enden av vanlig kriminalitetsbekjempelse, for da er det utlendinger i tillegg, altså i hvert fall i folks bevissthet, eller fremmede, og da er det da de andre. Fordi konsekvensene av de tiltakene vi setter i verk for å kontrollere «de andre» som ikke er oss, som egentlig rammer alle sammen og hele samfunnet, de er jo så utrolig abstrakte å forklare, og så usynlige, - man ser jo ikke at et demokrati forvitrer før det går ganske langt. Du ser ikke hvilke stemmer som blir borte i den politiske debatten, du ser ikke hvem som, hvilke krefter som blir marginalisert».*

Som Lund-kommisjonen i sin tid påpekte kunne det selv under normale, fredelige forhold ha negative konsekvenser. Mathiesen (2000) påpeker også bruken av registre til å lokalisere jøder i Norge under 2.verdenskrig. Vi har en enorm tillit til maskinene og systemene, men det er jo menneskene som styrer dem. På denne måten har tillit to sider og kan være farlig dersom man stoler blindt på institusjoner som politiet og rettsvesenet.[7]

> *«Det er en grunn til å tro at den elektroniske overvåkingen bare vil tilta, og at vårt eget ubehag vil melde seg som en forsinket grubling over hva det betyr at våre små og store hemmeligheter er på vandring der ute»* (Apenes, 2000 s.9).

En av mine informanter understreker at personvernet avhenger av at folk synes dette er viktig, og at folk ikke ser dette. Det er kanskje bare noen studenter, et par journalister og noen politiske aktive som mener at dette har direkte betydning for vår samfunnsform. Når dette er skjult for offentligheten har den politiske eliten mulighet til å sette sine planer ut i live uforstyrret, og kan til og med bidra til å spre frykt for fremmede eller kriminelle *andre* for å legitimere deres arbeid dersom det skulle være behov ressurser eller støtte i befolkningen (Loader, 2002). Dette kan også settes i sammenheng med panoptikken; det «sivile overvåkingsøyet» får i liten grad ta del i det myndighetene holder på med på dette området. Vi husker fra den panoptiske tankegang at overvåkingen kan være skjult, men man må være klar over at den er tilstede, selv om man ikke vet når den er til stede. Kan det være slik at den europeiske overvåking ikke har denne effekten siden de fleste ikke er klar over dens eksistens?

[7] Internasjonale undersøkelser har vist at Norge og Norden skårer høyere på tillit enn andre land i Europa (Wollebæk et.al, 2011). Lavt skårer Øst-Europa og USA kommer totalt dårligst ut.

Det kan i denne sammenheng nevnes at i et av mine intervjuer forteller Georg Apenes om hans forening som er startet opp – *Forening for Digitalt Personvern*. Man har her tatt «saken i egne hender» og ønsker å skape bevissthet rundt en sak som går direkte på folks personvern. På mange måter vil denne foreningen skille seg klart fra de typiske NGO's ved at det er en ren innsamlingsorganisasjon. Formålet er å kunne bistå med kapital til juridisk bistand dersom noen mener Datalagringsdirektivet strider mot de Europeiske menneskerettighetene og Grunnloven. Det er allikevel en forening som er fullstendig non-profit og også er drevet av engasjement fra de som arbeider med den.

Likevel er tendensen ofte at folk ikke i særlig grad er klar over det som foregår, og det er i hvert fall tilfellet for SIS. Uvissheten rundt dette fører kanskje til at det sivile blikket som burde vært mer til stede kan føre til at rettssikkerheten ikke i særlig grad blir ivaretatt. Ofte vil dessverre en slik sak som så mange andre først få publisitet når noe ekstremt og lite heldig har inntruffet.

6 Rettssikkerhet og personvern

Et av avhandlingens hovedtemaer er spørsmål som reiser seg rundt rettssikkerhet og personvern knyttet til informasjonssamarbeidet. Dette er et tema som ikke vil avta i aktualitet ved at SIS nå øker i kompleksitet ved lanseringen av SIS II.

I lys av rettssikkerhetsidealet og dets prinsipper vil jeg forsøke å ta Schengensystemet nærmere i øyesyn. Det er kun de sidene ved rettssikkerhet som er aktuelle for avhandlingen som her vil bli berørt. Det vil hovedsakelig bli tatt utgangspunkt i Ståle Eskelands (1988) forklaring og punktvise gjennomgang av begrepet *rettssikkerhet* og dets innhold. Jeg kommer også til å se nærmere på begrepet *personvern* og identifisere de farer informasjonssamarbeidet representerer.

Mine informanter har vært engasjert i dette og har kommet med fruktbar informasjon og interessante betraktninger.

6.1 Hva er rettssikkerhet?

Rettssikkerhet er et begrep som vanligvis brukes som en normativ karakteristikk for hvordan *forholdet mellom offentlige myndigheter og et enkeltindivid bør være* (Eskeland, 1988). Faren for at individers rettssikkerhet ikke er ivaretatt tilstrekkelig på grunn av det omfattende informasjonssamarbeidet har vært og er fremdeles et av de største ankepunktene knyttet til Schengen-samarbeidet.

Rettssikkerhet representerer det gode som ”alle” er for, men betydningen er ikke nødvendigvis entydig eller like enkel å gripe fatt i (Tamanaha, 2004). Man kan se rettssikkerhet som en beskyttelse av individers rettigheter, og mange vil mene at demokrati også er en viktig bestanddel i rettsikkerhetsbegrepet. Noen fremhever at det viktigste aspektet ved lovene er at de er formelle og generelle, og at de benyttes likt overfor alle. Rettssikkerhet vil også representere et hinder for maktmisbruk (Tamanaha, 2004).

«*Loven må være generell, lik og sikker*» (Hayel i Tamanaha, 2004). Med dette menes at lovene må være generelle på den måten at de ikke er rettet mot noen spesielle, men skal gjelde

likt for alle uten unntak. Sikkerheten ligger i at man på forhånd skal kunne vite hvilke lover som gjelder og på hvilken måte disse vil bli brukt.

Rettssikkerhet kan dreie seg om beskyttelse i forholdet *mellom* borgerne, men også som en beskyttelse *mellom borgerne og de offentlige myndigheter* (Eskeland, 1988). Det er dette siste som er mest aktuelt å se nærmere på her. Det viktigste i Schengens henseendet vil være den formen for rettssikkerhet som skal beskytte individet mot overgrep ovenfra - fra statsmakten. Det er etablert to skranker for forvaltningens adgang til inngrep hos borgerne; for det første for å sikre personlig integritet og likhet. Inngrepene skal også ha et rettslig grunnlag (Eskeland, 1988).

Rettssikkerhetsidealet innebærer at beslutninger som fattes skal tilfredsstille visse krav (Eskeland, 1988). Det skal også eksistere rettslige garantier for at avgjørelser fattes i henhold til disse kravene.

Man kan tenke seg at lovene frarøver individer frihet og legger føringer for hvordan vi skal opptre. Liberalismen bringer på banen den tanken at dersom alle er helt frie, så er man ikke fri egentlig, på grunn av den trusselen man kan representere for hverandre (Tamanaha, 2004). Ved å gi fra oss litt av friheten ved at vi underkaster oss for lovene, vil dette i seg selv gi oss større frihet totalt sett. Dersom lovene blir til i et demokrati skal de som lovene gjelder for også være utformerne av disse (Tamanaha, 2004). Spørsmålet er om overvåkingssystemene vi er vitne til i dag representerer noe særlig grad av frihet for enkeltindivider.

Kompleksiteten knyttet til rettssikkerhet øker når man opererer i et system som skrider utover landegrensene. Fra statens side kan det være vanskelig å oppfylle de overnevnte krav i et slikt system. Man har også en «bruker» som skal orientere seg i lovene og unngå å komme på kant med disse, og her er det viktig at dette følges opp og kommuniseres fra myndighetene på en god måte, og her ligger mye av kritikken. Det nevnes på generelt grunnlag at det er umulig for noe lovsystem å oppfylle alt dette (Hayel i Tamanaha, 2004).

6.2 Rettssikkerhetsprinsippene

Rettssikkerhet kan brytes ned i prinsipper som bør følges for å sikre at loven anvendes på et mest mulig likt og riktig grunnlag. Når man studerer et maskineri av Schengens kaliber vil man måtte ta i betraktning at lovene vil kunne ha en overlappende eller utflytende effekt utover landegrensene jfr. diskusjonen tidligere knyttet til rettslig pluralisme. Her vil jeg se nærmere på i hvilken grad rettssikkerhetsprinsippene tenderer til å være ivaretatt i Schengen-samarbeidet.

Rettsriktighet; avgjørelser skal være i samsvar med gjeldende rett (Eskeland, 1988). Dette er meget aktuelt knyttet til politisamarbeid som krysser landegrenser (Eskeland, 1988). Når lover gjennom globalisering og politisamarbeid flyttes over landegrenser kan det oppstå tvil om hvilket lands lover som til syvende og sist skal være gjeldene. Dette leder til en del nye utfordringer; hvem skal holde kontroll med og avgjøre hva som er gjeldende rett? Og hvordan skal et individ kunne orientere seg? Dette området leder oss tilbake til Mathiesens diskusjon knyttet til Lex Vigilatoria (Mathiesen i Deflem, 2008).

I følge Schengenkonvensjonen (2007) er det alltid landenes egne lover som skal være gjeldende. Det er altså ikke et overbygg av lover og regler som går inn for å overkjøre de nasjonale. Mon tro om dette nesten kunne vært et bedre alternativ for å forhindre stor forskjell slik at ikke samarbeidet drives på 26 forskjellige måter. På denne måten vil «maktesløsheten» ved at man får overnasjonale regler som «slår ut» de nasjonale kunne føre med seg en positiv effekt. Slik systemet fremstår i dag fører det til en ny form for pluralisme som er av en voldsom størrelsesorden når det finner sted innenfor et samarbeidende system. Dette vil igjen kunne føre til ulik praksis og at personopplysningers behandling vil kunne stå i større «fare» i noen land enn i andre.

Et annet problem man i Schengen-samarbeidet vil kunne komme ut for er «kontrollhull». Når eksempelvis Norge sender ut opplysninger via SIS følges ikke disse opp av det norske Datatilsynet. Spørsmålet er om noen vil følge opp der Datatilsynet slipper taket. Selv om det norske Datatilsynet følger sine plikter knyttet til kontrollen av SIS, kan dette være variabelt i andre land. Slik kan også et sett av opplysninger på ferden gjennom Schengen støte på flere lands lover, og vil kunne bli behandlet ulikt geografisk, etter gjeldende rett.

Verdiriktighet; Man skal ikke krenke et individ; skade dets psykiske og/eller fysiske integritet (Eskeland, 1988). Respekt for personlig integritet er et flertydig uttrykk og det gir rom for skjønn. Man kan selvsagt stille spørsmål om personlig integritet er ivaretatt i systemene dersom man registrerer ”myke” opplysninger som seksuell legning osv. På generelt grunnlag må det kunne sies at rom for skjønn kan representere et problem med tanke på tolkningsalternativer. Dette vil spesielt kunne gjøre seg gjeldende for SIRENE-systemet der den slags «myke» opplysninger kan registreres. Men man skal selvsagt heller ikke se vekk i fra muligheten for å tolke til det beste for et individ.

Rettskrav; krav til innsyn i saker som forvaltningen har til behandling (Eskeland, 1988). Alle skal kunne utøve kontroll og ha en kontrollfunksjon overfor forvaltningen ved innsyn. Et viktig prinsipp for denne typen kontroll er *offentlighetsprinsippet.* Allmennheten skal ha innsyn i offentlighetens saksdokumenter, og dette er et grunnleggende demokratisk prinsipp (Ny offentlighetslov, 2003:30). Dette er også et viktig prinsipp av rettssikkerhetsmessige hensyn. «*Kontroll motvirker maktmisbruk generelt*» (Ny offentlighetslov, 2003:30).

Som vist tidligere har man krav på innsyn i egne opplysninger, men dette vil falle vekk dersom det eksempelvis kan forringe en etterforsking. Data som politiet sitter på vil nok i de fleste tilfeller være langt vanskeligere å få innsyn i enn de fleste andre registre. Som nevnt er politiets arbeidsregistre ved dispensasjon fra Datatilsynet unntatt registerinnsyn (Mathiesen, 2000). På bakgrunn av dette kan det medføre riktighet å påstå at rettssikkerhetsprinsippet om krav til innsyn i stor grad vil falle vekk knyttet til SIS. Selv om man i utgangspunktet skal ha rett til innsyn vil det finnes såpass mange unntak at det er legitimt å påstå at individers rettssikkerhet knyttet til rett til innsyn i egne saker vil være dårlig. Dette er til dels forståelig knyttet til politiets virksomhetsområde, og man må velge mellom to onder.

Et annet punkt er at de fleste som befinner seg i et slikt system ikke er klar over dette, på denne måten vil de heller ikke kunne stille et slikt krav. Som Apenes uttrykker det:

> *«Det ligger dessuten en teoretisk kvalitetsgaranti knyttet til alle personregistre i det forhold at personene som er registrerte der har krav på å få vite hva som er registrert om dem og rett til å korrigere feil og ufullstendigheter. I praksis er det imidlertid ikke tilstrekkelig til å forebygge feil og unøyaktigheter simpelthen fordi det blir flere og flere personregistre og fordi det ikke er praktisk mulig for oss å vite hvor kunnskap om oss – korrekt eller ukorrekt – til enhver tid befinner seg»* (Apenes, 2000 s.26).

Det vil også ligge en viss grad av forskjellsbehandling i et slikt system. Brouwer (2008) viser til et eksempel der en registrert har forsøkt å få slettet sine opplysninger fra SIS fordi det er registrert på urettmessig grunnlag. Dette måtte gjøres ved omfattende advokathjelp, noe det er grunn til å anta at de færreste registrert i et slikt system vil kunne ha mulighet til å benytte seg av. På denne måten vil systemet innad kunne produsere «tapere» og «vinnere» på bakgrunn av eksempelvis økonomiske ressurser.

Eskeland (1988) nevner grunner til at data ikke bør veksles mellom organer. Data som er lagt inn med ett bestemt formål kan bli brukt til noe annet og det kan oppleves som krenkende at opplysninger om en ligger til andres skue (Eskeland, 1988). Dette vil være meget aktuelt med tanke på systemene som finnes i Schengen i dag der det er stor variasjon landene i mellom med hensyn til hvilke organer som har tilgang. Selv om det i Norge foreløpig kun er Kripos som har tilgang til hele systemet og UDI til deler av det, er ikke dette representativt for resten av medlemslandene. Som vist tidligere kommer det flere og flere systemer til og de knyttes opp til SIS i større utstrekning. Dette kan føre til at en opplysning som i utgangspunktet er lagt inn i SIS kan ende opp i andre registre og databaser, og dette kan sette opplysningene i ytterligere fare. Muligheten man har som enkeltindivid til å ha kontroll på hvor ens opplysninger befinner seg virker umulig.

Rettssikkerhet innebærer også et element om *likhet* og *rettferdighet* (Eskeland, 1988*) "Alle som dekkes av den samme regel skal behandles likt"* (Eckhoff i Eskeland, 1988). Likhet for loven er et velkjent begrep. Men mon tro om alle har like stor sjanse for å havne i registrene? Har alle like store muligheter for å bli overvåket? Det hjelper ikke hvis hele grupper av mennesker blir behandlet likt dersom dette skiller dem fra andre grupper. Her er man inne på stigmatisering av grupper og enkeltindivider.

På individnivå kan man med tanke på registreringsalternativene som uskyldig bli dratt med i «dragsuget» dersom man eksempelvis befinner seg sammen med en person politiet er ute etter. Dette finner man i Schengenkonvensjonens (2007) art.99 pkt. d: *Persons accompanying the person concerned or occupants of the vehicle.* Dette kan medføre at uskyldige personer får en oppføring i SIS.

Rettssikkerheten kan stå i fare ved at lover globaliseres slik vi er vitne til i dag. Globaliseringen fører også til at vårt eget rettssystem endres. Dette er temaer som berøres ved at vi har gått inn i et internasjonalt samarbeid.

> *«… er det noen større rettssikkerhet… altså det er jo noen regler for Schengen og hva som kan registreres i systemene, men jeg må ganske enkelt spørre: hva er det som er rettssikkerheten rundt de systemene? De som blir registrert i systemene har jo ikke mulighet til å ta til motmæle…».*

Min informant påpeker at én ting er å registrere en opplysning, det neste i eksempelvis et arbeidsregister, som tidligere har hatt sine konsekvenser, for så å iverksette andre mer inngripende tiltak som avlyttinger og liknende. Han mener at mer overvåking kan ødelegge den gjensidige tilliten i et samfunn. Dette var også en del av det som lå bak Lund-kommisjonen i sin tid. Det var blitt en grunnleggende mistillit på politisk nivå som skyldtes rykter og mistanker knyttet til de hemmelige tjenestenes virksomhet. Helt uavhengig nevner også min informant fra EDPS viktigheten av at myndighetene opererer med rettssikkerhet in mente og at dette fostrer tillit i samfunnet. *Databeskyttelse fostrer tillit*. Som Apenes skriver er tillit en av de viktigste bestanddelene i vårt samfunn, men den savnes gjerne først når den er vekke og det er for sent (Apenes, 2000). Tillit er en av de mest essensielle komponentene i vårt samfunn.

> *«Det er alltid grupper som vil føle seg spesielt uthengt i sånne sammenhenger, spesielt gjenstand for denne overvåkingsinteressen. Og det kan bli svære grupper i Norge… blant annet muslimer».*

Man kan trekke paralleller fra Lund-kommisjonen og frem til i dag; man tok sikte på en total registrering av alle som var kommunister i Norge. Disse ble registrert i overvåkingstjenesten og det ble utvekslet opplysninger. Dette hadde betydning for deres yrkesmuligheter, og noen fikk vanskeligheter som følge av dette. Som min informant beskriver har Norge trukket fordeler av all verdens urettferdigheter, men man kan jo tenke seg at situasjonen vil endre seg. Hvis samfunnet blir satt under stress, vil vi vende oss mot alt som er annerledes. Dette kan også bygge opp under tankene jeg har rundt stigmatisering. Kan dette bety at registrene har potensial til å kunne bli ekstra farlige?

Demokrati er som nevnt en viktig del av rettssikkerhet, der man skal ha mulighet til å debattere og bli informert om det som foregår. SIS II har blitt til bak lukkede dører som gjør at man ikke har kunnet ta del i prosessen (Parkin, 2011b). SIS II blir av Parkin omtalt som et system som har blitt til mer under en «nødsituasjon», og det har vært stort press fra politisk hold. Systemet vil nå inneholde et sett av langt mer kompliserte og omfattende biometriske data, så fallhøyden når det gjelder rettssikkerhet er nå langt større enn tidligere (Parkin, 2001b). De etiske aspekter som reiser seg rundt et slikt system har ikke vært tatt særlig

hensyn til i utviklingen av SIS II, og dette må settes i høysetet i fremtiden (Parkin, 2011b). Tidspresset kan ha ført til at fokuset på sikkerhet og etiske aspekter har kommet i annen rekke. For å sikre systemet mot manuelle fallgruver bør man i slike systemer bygge inn såkalt «data protection by design», der man eksempelvis kan legge inn automatiserte løsninger for sletting av data når det er tidsmessig riktig, i stedet for at dette skal overlates til brukerne av systemet (Parkin, 2011b).

Parkin (2011b) mener i tillegg at en uavhengig vurdering må til for å vurdere om SIS II vil ha ønsket betydning med hensyn til å øke sikkerheten i Europa. Man må sette nødvendighet, proporsjonalitet og fundamentale rettigheter opp mot hverandre. SIS II har ennå ikke kunnet vise til å være et sikkert system (Parkin, 2011b).

På systemnivå ser det likevel ut til at rettssikkerhet er et tema som ikke har passert fullstendig. Schengenområdet kan sammenliknes med Euro-sonen; hvis problemer oppstår ett sted kan dette smitte raskt (Marini, 2011). Dersom et av landene ikke har systemene i orden og rettssikkerheten er på hell kan dette ha store ringvirkninger som vil gå utover alle de andre medlemslandene i Schengen (Marini, 2011).
Bulgaria og Romania kom med i EU i 2007, men har likevel ikke fått medlemskap i Schengen-samarbeidet (Calabrese, 2011). Årsaken til dette er at disse to landene har en lang vei å gå med hensyn til å utbedre sine rettssystemer, men det ser ut til at hovedvekten av beslutningen er tatt på bakgrunn av korrupsjon og at Schengengrensene som da vil utvides østover vil kunne skape store problemer. De vil stå sammen for å kontrollere disse grensene. Disse to landene er høyt utsatt for trafficking og organisert kriminalitet og det vil kreve mye av disse som medlemsland om dette skal kunne fungere (Calabrese, 2011). De blir altså sett på som «svakere ledd» på flere områder, og holdes som årsak av dette ute fra Schengen-samarbeidet. Dette tyder på at man har in mente at man skal ha visse standarder som medlem når det gjelder rettssystemet, og dette taler til fordel for rettssikkerhetens ivaretakelse. Et annet spørsmål er om disse landene vil kunne klare å utbedre dette med tanke på den økonomiske situasjonen de står i.

6.3 Personvern

Personvern kan sees i sammenheng med individers rettssikkerhet, men personvern er noe mer spesifikt. Som en av mine informanter påpeker har vi aldri vært så registrert og overvåket foruten om i det gamle byborg-samfunnet. Var man fredløs og bodde utenfor murene var man ikke overvåket, men på innsiden var samfunnet nokså gjennomsiktig. Vi som lever på innsiden av «Schengen-murene» er utsatt for overvåking, noen grupper mer enn andre. Spørsmålet som reiser seg er i hvilken grad personvernet ivaretas, og hvordan man skal bøte på eller forhindre de negative konsekvenser dette kan føre med seg.

6.3.1 Hva betyr egentlig personvern?

«Personvern» er ikke et begrep som er enkelt å definere og personvern kan oppfattes forskjellig fra individ til individ (Datatilsynet.no, 2011a 25.11.2011). «Personvern» kan forklares som retten til et privatliv og ens rett til å bestemme over egne personopplysninger. Begrepet vil også innebære at man har rett til en privat sfære som man selv bestemmer over uten noen form for innblanding fra andre, dette inkluderer også innblanding fra staten (Datatilsynet.no, 2011a 25.11.2011).

Retten til et privatliv er nedfelt i den Europeiske menneskerettighetskonvensjonen, men det finnes ingen regler uten unntak (European Convention on Human Rights, art.8):

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

Personvernet har også et viktig samfunnsmessig formål, som er viktig for å sikre felles goder i et demokratisk samfunn (Datatilsynet.no, 2011a 25.11.2011). Dersom personvernet ikke ivaretas på en ordentlig måte kan dette føre til at representanter fra sivilsamfunnet vil vegre seg fra å delta i politisk aktivitet og meningsutvekslinger, fordi man frykter at dette kan bli benyttet mot en og gjort til offentlig skue. Dette vil i særdeles stor grad gjelde lagring av informasjon i ulike registre (Datatilsynet.no, 2011a 25.11.2011). Man trenger ikke se lengre

enn til nyhetssendingene der de som gjør opprør i gatene og ytrer sine ekstreme holdninger er nøye iakttatt av politiet. Det er nok noe naivt å tro at denne iakttakelsen bare er i form av fysisk tilstedeværelse.

6.3.2 Personvern i SIS

En av mine informanter påpeker viktigheten av åpenhet, forutsigbarhet og en mulighet for å kunne gjøre bevisste og selvstendige valg. Individets frihet og bestemmelsesrett til å la seg registrere er i ferd med å forsvinne da vi har mistet samtykket for de fleste registre. I sammenheng med SIS er selvbestemmelsesretten fullstendig uteblivende.

Når det gjelder registrering vil en god ivaretakelse av personvernet tilsi at man skal registrere minst mulig, altså kun det som strengt tatt er *nødvendig*, og det bør også basere seg på samtykke så langt det er mulig fra den som registreres (Datatilsynet.no, 2011b 30.12.2011). Dersom behandlingen av personopplysninger ikke foregår under et informert samtykke må det foregå på et *rettslig grunnlag* (Datatilsynet.no, 2011b 30.12.2011). Det er dette siste som vil være gjeldende for SIS. På denne måten vil man alltids kunne ha hjemmel til å se vekk i fra personvernmessige hensyn så lenge man har loven på sin side. Man blir ikke informert når man blir registrert i SIS, og dersom man får vite om dette er det gjerne for sent eller svært vanskelig å gjøre noe med (Brouwer, 2008).

Det er også viktig at registreringen av opplysninger er *proporsjonalt* med formålet (Datatilsynet.no, 2011b 30.12.2011). Det må være en viss proporsjonalitet mellom sak og registrering. For å sette det på spissen; det vil være lite formålstjenlig å registrere seksuell legning i skattelistene. Det er viktig at man alltid vil velge det alternativet som er minst inngripende overfor et enkeltindivid når man skal samle inn personopplysninger. Det er viktig at overskuddsinformasjon og irrelevante opplysninger unngås (Datatilsynet.no, 2011b 30.12.2011). Man er nødt til å skille mellom «need to know» vs. «nice to know». Det påpekes også av Datatilsynet at det skal være knyttet en *formålsbestemthet* ved opplysningene; det vil altså si at de ikke skal benyttes til annet formål enn det de var samlet inn for (Datatilsynet.no, 2011b 30.12.2011). Nettopp dette faremomentet har SIS mottatt stor kritikk for. Man skal ikke lagre informasjon på måfå, og informasjon det ikke lengre er behov for skal slettes. Det

er også svært viktig at politiet gjør en vurdering av viktigheten før man legger inn opplysninger eller en varsling i SIS (Brouwer, 2008). Dette må gjøres etter den såkalte «klausulen om proporsjonalitet» som først nevnes i reguleringen av SIS II (Brouwer, 2008). Dette blir igjen et område som vil bli overlatt til skjønnsmessige vurderinger, og forskjeller i praksis vil meget trolig forekomme.

Generelle tekniske krav til informasjonssikkerhet er et viktig ledd i ivaretakelsen av personvernet (Datatilsynet.no, 2011b 30.12.2011). Man må også sikre at opplysninger er korrekte (Datatilsynet.no, 2011b 30.12.2011), da det kan få fatale konsekvenser for et enkeltindivid om det fattes beslutninger basert på feil informasjon. Flere av disse forholdene nevnes også i Schengenkonvensjonen kapittel 3; «*Protection of personal data and security in the Schengen Information System»*. Her påpekes viktigheten av logging, samt at det ikke er tillatt med kopiering fra systemet annet enn på systemteknisk grunnlag (Schengenkonvensjonen, 2007 art.102). Man kan for eksempel ikke kopiere en bit informasjon og legge dette inn i en nasjonal database.

Det er også saneringsregler for når informasjon skal fjernes fra SIS. Disse er noe vanskelig å gripe fatt i, og det kommer også an på hva slags type opplysninger det gjelder. For en privatperson vil det kunne være helt umulig å få innsyn i om saneringsreglene overholdes. Den overordnede regelen er *at persondata ikke skal oppbevares i systemet i lengre tid enn det er behov for å oppnå målet med at de ble lagt inn* (Schengenkonvensjonen, 2007 art.112). Dette gjelder spesielt når formålet er sporing av personer. Den staten som har lagt inn opplysningene skal senest 3 år etter at de ble lagt inn gjøre en vurdering på om opplysningene kan fjernes. For å kunne overholde dette skal det fra teknisk support bli gitt varslinger en måned før informasjonen bør vurderes. Man kan ut i fra landets egne nasjonale lover sette kortere intervaller for når man skal ta opp varslingene til vurdering (Schengenkonvensjonen, 2007 art.112). På bakgrunn av dette vil enkelte land nok ha bedre kontroll og en mer oppdatert database enn andre.
Man har mulighet til å forlenge perioden for oppbevaring av opplysningene i SIS (Schengenkonvensjonen, 2007 art.112). Data som slettes fra SIS vil likevel holdes lagret av teknisk support ett år etter sletting (Schengenkonvensjonen, 2007 art.113). Det er nedsatt en maksimal tidsramme på 10 år for lagring av opplysninger, samt ett år i tilleggs-lagring av teknisk support (Schengenkonvensjonen, 2007 art.113). Etter dette må dataene destrueres.

I praksis, tatt smutthullene i betraktning for lagring av informasjon, kan informasjonen lagres på ubestemt tid så lenge man anser behovet til stede. Det er nærliggende å anta at en del informasjon kan være nyttig å beholde lagret i *tilfelle* man får behov for den. Det blir en skjønnsmessig vurdering som nok er vanskelig, og kan føre til «over-lagring» i et forsøk på å sikre seg for fremtidige hendelser jfr. morgendagens risiko. Det er antakelig også et spørsmål om kapasitet og i hvilken grad man har mulighet til å gå inn på hver enkelt oppføring og gjøre en slik vurdering. Man kan på bakgrunn av dette stille spørsmålet om SIS inneholder en del opplysninger som faller litt mellom flere stoler. Spesielt med tanke på at man kan forlenge tidsperioden for opplysningenes eksistens i SIS.

Noe som likevel taler i opplysningskontrollens favør er det faktum at antallet registreringer i SIS sank med 7,4 % fra 2007 til 2008 (Brouwer, 2008). Dette forklares ved at man måtte trekke tilbake opplysninger når nye land ble medlem av Schengen og personer fra disse nå kunne ferdes fritt i Schengenområdet (Brouwer, 2008). Dette tyder på at man har hatt forholdsvis god kontroll med opplysningene og kan gjøre en slik justering. Det reiser imidlertid spørsmål knyttet til hvorfor man hadde registrert disse opplysningene når de tilsynelatende var av en så «verdiløs» karakter at de kunne slettes «uten videre». Disse personene fikk nå altså tilgang til Schengenområdet, men det kan være tegn på at de var registrert på et noe bagatellmessig grunnlag. Dette blir selvsagt bare spekulasjoner og baserer seg kun på betraktninger.

Informasjonen kan heller ikke bli benyttet til rent administrative formål. Schengenkonvensjonen er mer konkret enn man kanskje kunne forvente av et slikt dokument, men gjennomgående henvises det til nasjonale regler som igjen vil føre til ulikhet i praksis. Selv om det er et inngripende forslag kan man selvsagt reise spørsmålet om det ikke ville vært mer fordelaktig å ha overnasjonale regler som ville overstyre de nasjonale lovene på noen punkter når man først er med i et slikt samarbeid for å forhindre ulikhet som nevnt tidligere.

Artikkel 111 i Schengenkonvensjonen (2007) understreker at dersom en domstol beslutter at opplysninger i SIS skal endres eller fjernes skal de ulike partene i Schengen innrette seg etter dette. Brouwer (2008) påpeker at det er bekymringsverdig at de nasjonale datatilsynene kun har rapportert et fåtall av forespørsler om retting eller sletting av data til JSA. Hun mener dette indikerer at tilsynene ikke er tilstrekkelig informert om de utfordringene som SIS reiser og de utfordringene privatpersoner har knyttet til dette (Brouwer, 2008).

Det kan heller ikke påpekes for ofte at det er store utfordringer knyttet til utveksling av informasjon *mellom* ulike databaser. Man har i EU satt i stand en Information Management Strategy (IMS) som ser nærmere på datasikkerheten og personvernet i Europa (Töpfer, 2011). IMS ble godkjent samtidig med Stockholm-programmet[8] i 2009. Man har også sett på «privacy by design»; altså at man kan forme de tekniske løsningene slik at man ivaretar personvernet (Töpfer, 2011). Det er nærliggende å anta at i utvekslingen mellom ulike databehandlere vil opplysninger kunne være ekstra utsatt samtidig som spredningen er et risikomoment i seg selv. European Informations Exchange Model (EIXM) er også et ledd i å sikre og få mer kontroll på utvekslingen av opplysninger mellom organer (europa.eu 25.3.2013). Man ønsker med dette pågående arbeidet å kartlegge informasjons- og kommunikasjonsstrømmen, samt de ulike tekniske løsningene som er i bruk (europa.eu, 25.3.2013).

Likevel er det ingen overdrivelse å si at registrene som politiet benytter faller utenfor de alminnelige prinsippene for personvern. Datatilsynets fritakelse fra registerinnsyn med alt det dette innebærer som vist tidligere, samtidig som det er en underliggende tro på at formålet helliger middelet, gjør dette til et felt med mange utfordringer for personvernet.

Man kan også se det slik at har man ikke noe å skjule har man ei heller noe å frykte. Registrering av opplysninger har også utvilsomt sine fordeler, men det er misbruket, de store konsekvenser av feil, ulikheter i bruk og unødvendig registrering som må sies å være de største ankepunktene. Har man ved en feil havnet i et slikt register vil veien ut kunne være lang og tung og vil kunne kreve midler majoriteten ikke har til rådighet.

6.3.3 Personvern – den tid den sorg?

Globalisering er en viktig faktor; handel øker på verdensbasis, data flyttes over landegrensene og internasjonale transaksjoner øker. Internasjonalt politiarbeid har også ekspandert de siste årene. Alt dette krever en lov som sikrer personvern og datasikkerhet i større grad enn tidligere. Utviklingen går så raskt at det er nærliggende å tro at det er en stor utfordring og

[8] Stockholm-programmet søker å ivareta EU-borgeres sivile rettigheter og personvern med fokus på rettferdighet, sikkerhet og frihet. Innsyn i dokumenter for sivile er et viktig punkt på agendaen (europa.eu 23.3.2013).

predikere problemene før de har oppstått. Spørsmålet er hvor enkelt det er å ivareta personvernet.

Min informant fra EDPS understreker at vi nå er inne i en helt annen æra. Den største utfordringen for datasikkerhet og personvern er den teknologiske utviklingen; vi står nå overfor nyvinninger slik som «cloud computing», sosiale nettverk, adferdsstyrt annonsering og stedtjenester. Dette har endret seg betraktelig og svært raskt, og er sterkt knyttet til hvordan personvern tolkes og praktiseres. Har vi ikke klart å forutse og predikere de problemene som ville måtte komme som et resultat av en slik utvikling? Mye av det som ligger til grunn for reglement knyttet til sikring av opplysninger som benyttes i EU i dag ble forfattet på 80-tallet (Boehm, 2009). Med den raske utviklingen vi har vært vitne til vil man ikke med disse reglene være rustet for dagens trusselsituasjon når det kommer til datasikkerhet.

Apenes setter et bilde på IT-revolusjonen knyttet til personvern som kan virke nokså beskrivende; det kan sammenliknes med en skredfare; det er vanskelig å predikere når og hvor skredet vil gå, og hvor langt det vil gå (Apenes, 2000). Flere av mine informanter ser det slik at denne «skredfaren» først blir tatt hensyn til når det begynner å bli for sent. En av mine informanter ser det som et grunnleggende systemproblem at man gjerne kommer haltende litt etter med det man mener er viktige hensyn og formelle vedtak for å lappe på de hullene som har oppstått.

> *«… det blir liksom litt sånn papirorden på det, fordi det er… inntrykket er og det ser jeg mest gjennom små dryppeksempler (…) det er ikke noe særlig kontroll på det. Det flyter ganske fritt. Og det er ikke så mange som kan fortelle deg hvor tingene ligger og hvem som har tilgang til enhver tid til opplysninger.»*

Min informant legger ikke skylden på eksempelvis Kripos, selv om han understreker at det ikke ville skadet om de prøvde å se litt utenfor «boksen», men skylden bør legges på de som styrer det hele fra toppen av hierarkiet.

> *« (…) samtidig så aksepterer jeg at de har en jobb, de er en sektor, det er egentlig systemets oppgave å sørge for at de, ja, de er en stemme, de kommer med sine behov, med større eller mindre skylapper for andre hensyn, skal ikke skylde på dem, men jeg skylder på de som skal koordinere alt – at de har tillatt at det er de hensynene og de synspunktene som i veldig stor grad har fått prege resultatene hittil».*

Min informant påpeker at inntrykket han sitter med er at personvernet blir ivaretatt forholdsvis dårlig. Siden terror i så stor grad er satt på dagsorden blir innvandring og terror

raskt knyttet sammen. Man har i liten grad vært opptatt av å bake inn og utrede konsekvenser for personvern. Dette har ofte kommet i ettertid fra myndigheter som har dette som oppgave, men som ikke har blitt hørt før tingene er på plass. Da først peker man på manglene og starter *reparasjonsprosessen*. Det påpekes at det verste er at de myndighetene som faktisk har en institusjonell oppgave i det formelle forvaltningssystemet både i EU og nasjonalt ikke blir hørt godt nok i disse prosessene. Man er helt avhengig av at man tenker beskyttelse av personopplysninger fra starten av når man lager et system eller et register, ikke når man ser hva man har endt opp med. Begynner man med dette for sent blir situasjonen helt uoverskuelig og ofte for dyr til at man har mulighet til å gjøre noe med det. Dette er også viktig av hensyn til rettssikkerheten. Dette kan også settes i sammenheng med de store forsinkelser man har fått i ferdigstillelsen av SIS II; alle forhold var ikke utredet i utgangspunktet som resulterte i enorme forsinkelser.

En av mine informanter nevner utfordringene ved at når man utreder forhold knyttet til dette så er man ikke flink til å inkludere uavhengige instanser, i den grad de overhodet tar forhold knyttet til personvern i betraktning. Man har en tendens til å tenke at «dette har vi kontroll på». Min informant anser dette som en «høflighetsvisitt» til et hensyn uten at det blir utredet grundig. Det understrekes at man har mange høringsinstanser, men det er noe annet enn å faktisk involvere offentlige eller sivile som sitter med en kompetanse som kan være avgjørende i dette arbeidet. Et eksempel her kan være Datatilsynet som ikke i særlig grad ble involvert da Norge gikk inn i Schengen-samarbeidet. Et forslag her er å i større grad ta i bruk privat ekspertise, selv om dette ofte omtales i negative ordelag. Da vil man i hvert fall kunne få et mer nøytralt syn på det hele. Ikke-statlige organisasjoner (NGO's) som engasjerer seg i personverndebatten bør også inviteres til å komme med uttalelser.

En av mine informanter påpeker som et av de verste problemene den situasjonen som kan oppstå ved at man i samfunnet begynner å føle seg maktesløs som individ. At man føler det er noe mye større enn en selv som vet mye mer om enn selv enn det en selv gjør. Her penser vi igjen inn på *tillit* som et av de viktigste bestanddelene i et samfunn. Samfunnssikkerheten er minst like avhengig av sivilsamfunnets samhold og tillit til hverandre. Den økende grad av registrering kan føre til at man blir redd for å blande seg inn, selv i de situasjoner der det er nødvendig, fordi man er redd for hva man bli trukket inn i og de problemene dette kan skape. En av mine informanter mener dette kan være psykologisk nedbrytende for et samfunn.

Min informant fra Datatilsynet mener det ikke er mange grunnene til å være optimistisk med tanke på personvern i tiden fremover. Men Datatilsynet har dette på agendaen, og takket være at folk flest blir vant til personverninnstillinger i ulike sosiale medier som Facebook så blir man klar over at dette finnes og det gjøres til allemannseie. På denne måten mener min informant vi har en større forankring av personvernbegrepet nå, men dette gjelder kanskje bare knyttet til temaer som befolkningen har en nærhet til. Datalagringsdirektivet har også bidratt til å sette dette mer på dagsorden og fått oss til å tenke over i hvilken grad man godtar å bli registrert. All overvåking har et gode, og ved å kunne avdekke pedofile eller terrorister vil de fleste mene at det meste er greit. Men overvåkingen har også sin bakside.

EDPS understreker overfor meg at det er avgjørende at man finner en balanse mellom personvern og sikkerhet. Min informant mener databeskyttelse og personvern ofte feilaktig sees på som et hinder som står i veien for arbeidet med å beskytte individers sikkerhet. Det er også viktig å være klar over at skal man kunne opprettholde en viss form for sikkerhet vil også noe måtte ofres. Spørsmålet blir snarere i hvilket omfang og til hvilken pris. Det henvises til Menneskerettighetskonvensjonen partikkel 8 der det understrekes at politiet og myndighetene generelt kan benytte data som er relevant for deres arbeide, men ikke ubegrenset. Man må ha en balanse mellom nytte og proporsjonalitet. Noen vil imidlertid mene at for at man skal kunne drive en stat er man helt avhengig av å vite noe om hvem som befinner seg i den, og det at man vet litt om folk ikke spiller så stor rolle. Informasjon kan være svært verdifull, ellers ville man ikke samlet den, men man må være klar over at man dessverre ikke bare får servert medaljens fremside i et slikt system. Slik situasjonen er nå balanserer Schengen-samarbeidet i en svært vaklende gange mellom nytte og de konsekvenser dette har for individer.

Når mye av reglementet for personvern og rettssikkerhet har bygget på til dels gammelt og utdatert materiale representerer Lisboatraktaten på den annen side et glimt av positivisme i det hele. Lisboatraktaten som ble underskrevet av EU landene i 2007 ser Europa i et nytt lys og tar i større grad med i beregningen at vi nå ikke befinner oss i den samme æra som tidligere (europa.eu 19.3.2013). Den tar blant mye annet sikte på å håndheve sivile rettigheter og beskyttelse av EU's borgere. Vet et nærmere øyekast går traktaten imidlertid ikke i dybden på beskyttelse av personopplysninger og personvern.

Behovet for ivaretakelsen av personvern blir ikke mindre nå etter at SIS II er lansert. Når også barn kan entres systemet som vist tidligere reiser dette også spørsmål knyttet til personvern.

Barn skal riktignok legges inn i systemet hovedsakelig i fall det er savnet, men mon tro om man kan bli lagt inn i SIS dersom man er i følge med en ettersøkt eller uønsket voksen. Dersom dette er tilfellet vil dette kunne føre til at uskyldige allerede fra barneårene kan bli lagt inn i SIS. De rettigheter myndige personer vil kunne ha mulighet til å håndheve vil av naturlige årsaker ikke gjelde for barn. Her må man klamre seg fast til nytten systemet kan ha med hensyn til bortføringssaker og liknende, og håpe at sikkerheten er til stede slik at faren for misbruk av opplysninger er minimal. Driftingen av SIS gjøres som nevnt tidligere av private aktører. Dette kan ha både fordeler og ulemper for sikkerheten av personopplysninger.

6.4 Informasjon som valuta

Som vist tidligere har globaliseringen ført med seg at flyten av varer, mennesker og handelen på verdensbasis har økt. Men det kan se ut til at denne handelen har spredt seg til en ny og mer skjult form for varehandel; «handel» med informasjon på et internasjonalt nivå.

For å opprettholde gode samarbeidsvilkår i et internasjonalt politiarbeid og samtidig få det man trenger av informasjon samlet inn av samarbeidende parter må man også kunne ha noe å tilby. Min informant nevner et eksempel hentet fra blant annet Datalagringsdirektivet for å eksemplifisere datahandelen på det internasjonale «markedet».

> *«FRA- loven i Sverige – et system som overvåker all elektronisk kommunikasjon som passerer Sveriges grenser(…) Man kan gjøre bestemte søk basert på bestemte søkekriterier for å verne rikets sikkerhet. Det er et drastisk tiltak i et demokrati. Da sa Karl Bildt rett ut at hvis vi skal være med å samarbeide med de store, så må vi ha noe å gi dem. Altså rett og slett; da må vi ha noe informasjon å handle med. Og det samme sa faktisk Janne Kristiansen i forbindelse med Datalagringsdirektivet – at hvis vi skal forvente noe igjen fra våre samarbeidende tjenester så må vi ha noe å gi dem».*

Det er relativt oppsiktsvekkende at man sier det rett ut på denne måten. Min informant mener at mange ser på Europeisk personverntenkning som overmåte streng, men det er jo nettopp fordi man ønsker å holde en slags kontroll med hva informasjonen blir benyttet til, og at folk ikke skal føle en stor uvisshet omkring hvem som vet hva om dem.
Et annet eksempel på informasjonsflyten er etterretningstjenesten (e-tjenesten). Informasjonen flyter, og det understrekes fra min informant at her utveksles det mye uformelt og vagt regulert.

Igjen kan relevansen av rettspluralisme reises. Man benytter hverandre også i større utstrekning enn tidligere når man er med i et slikt samarbeid. Problemer reises når regelverk flyter inn i hverandre og kontrollen forringes. Hvilke regler som til slutt gjelder kan bli en forvirrende affære å gjøre seg kjent med og man kan også utnytte dette til egen gevinst.

> *«Samarbeid er én ting, men hvis det blir for sammensmeltet så man ikke vet hvilket regelverk som gjelder og… så er det fort en fare for at man bruker hverandre og sier «kan ikke dere få tak i den informasjonen, for vi kan ikke» og i de kretsene der er det ingen politiker som kan hevde at det er noen særlig kontroll med hvordan opplysninger flyter der og flyter ut av Europa og når du er på det nivået, med myndigheter i land der det absolutt ikke er noen hyggelig tanke nødvendigvis for den det gjelder at opplysninger ender opp.»*

Dersom man omgår egne lands regler for å samle inn informasjon, samtidig som man benytter seg av informasjon innhentet fra samarbeidende parter blir dette et svært uoversiktlig terreng. Jeg viser igjen til Belgia som fikk sine svenske kolleger til å drive telefonavlytting, da dette ikke er tillatt etter belgisk lov.

6.4.1 Tilgjengelighetsprinsippet

Informasjonen skal flyte, og den skal flyte enkelt og effektivt. *Tilgjengelighetsprinsippet*, eller «*principle of availability*» henviser som vist tidligere til prinsippet om at all informasjon skal gjøres tilgjengelig for samarbeidende stater dersom det er behov for dette eksempelvis i etterforskingsøyemed (Kvam, 2008). Dette vil presentere et «fritt marked» for informasjon (Bunyan, 2006). Ved at alle har tilgang til alt i alle databaser vil dette føre med seg store konsekvenser for personvernet. Og det er i denne retning utviklingen går.

Det å holde kontroll med flyten av informasjon vil være meget vanskelig, for ikke å si umulig, og sjansen for misbruk øker. Samarbeidende parter utenfor EU vil også sannsynligvis etter hvert få tilgang til informasjonen (Bunyan, 2006). På denne måten vil informasjonen på under en brøkdel av et sekund kunne befinne seg utenfor Europas grenser, og Schengens og de europeiske lands reglement ligger igjen på grensen.

Hague programmet lister opp prinsipper som informasjonsflyten skal følge og beskriver også «principle of availability».

Her følger utdrag fra de nevnte prinsipper fra pkt. 2.1 *Improving the exchange of information*:

> *1) the exchange may only take place in order that legal tasks may be performed.*
> *2) the integrity of the data to be exchanged must be guaranteed.*
> *3) the need to protect sources of information and to secure*
> *the confidentiality of the data at all stages of the exchange,*
> *and subsequently,*
> *4) common standards for access to the data and common*
> *technical standards must be applied.*
> *5) supervision of respect for data protection, and appropriate*
> *control prior to and after the exchange must be ensured,*
> *6) individuals must be protected from abuse of data and have*
> *the right to seek correction of incorrect data.*

Selv om det er vel og bra at man identifiserer og forsøker å håndheve regler for «spillet» er det mye som tilsier at jo flere som har tilgang, jo mer informasjonen spres, og om den i tillegg kommer utenfor Europa så vil faren for at individers rettssikkerhet og personvern blir skadelidende øke.

Det at informasjon om mennesker bevisst eller ubevisst blir sett på som en «vare» som kan byttes inn for nye «varer» kan føre til at man mister forståelsen av hvor dyrebar og ikke mist skjør informasjon om personer er. Og jo større samarbeidet blir i og utenfor Europa, jo større blir denne faren. Dette er en skummel utviklingstrend som tilsynelatende vil undergrave de fleste positive tiltak med hensyn til ivaretakelsen av personvern.

Det skal understrekes at ved at dette systemet er så lukket som det faktisk er, er det ingen systematiske undersøkelser som har blitt gjort utover de kontrollene som føres fra myndighetene, eksempelvis Datatilsynet. Til det er systemene underlagt for stor grad av hemmelighold. Det blir på denne måten ikke mulig å si noe med sikkerhet angående situasjonen rundt personvern i SIS, men basert på de forhold som jeg har presentert er det grunn til å mene at det er et stort utviklingspotensial som bør følges opp.

7 Effekten av Schengen-avtalen

Schengen-samarbeidets hovedformål er som vist å holde uønskede inntrengere ute fra Schengenområdet, mens Schengens borgere kan reise passfritt, enklere og mer effektivt. Som vist har Schengenmaskineriet ført med seg spørsmål knyttet til datasikkerhet, personvern og rettssikkerhet. Men har man oppnådd det man ønsket med avtalen?

7.1 Schengen som problemskaper

> *«Man kan spørre hvor effektivt virker det som skal beskytte EU's grenser ut mot tredjeland, og der har jeg inntrykk av at dette kan være nokså lempfeldig. Dette med fri flyt også av personer har jo fått en religiøs betydning også innenfor EU-samarbeidet».*

Har man med Schengen-samarbeidet klart å leve opp til de målsettinger man opprinnelig hadde, eller har dette utviklet seg og gått i en helt annen retning?

Av mine intervjuobjekter har mine informanter fra Kripos vært de som har hatt størst kunnskap om å uttale seg om de direkte effekter Schengen og spesielt SIS har hatt på flyt av personer og kriminalitetsbekjempelse i Europa.

Mine informanter i Kripos er vel bevisst på at SIS er et kompenserende tiltak for nedbyggingen av de indre landegrensene og kontrollen av denne. Kripos understreker at man *har hatt stor nytte av SIS og antallet etterlysninger og treff har økt.* Tilgjengeligheten til SIS er bra og et stort antall sluttbrukere i politiet kan søke ut informasjon. Dette ser Kripos på som positivt, selv om dette som tidligere nevnt er et av de største ankepunktene knyttet til systemet. Det er noe kontroversielt at det som på innsiden av systemet ses på som positivt og helt avgjørende for systemets suksess av utsiden vurderes som de største farene og problemene. Det kan virke som om man sitter på hver sin tue med sitt spesialfelt, og det er få som har evne eller kunnskap til å kunne se helheten.

Jeg reiser spørsmål om antall søk har økt fordi man har fått mer flyt av mennesker, eller om det har økt fordi man nå har et lett tilgjengelig system å søke i. Jeg blir gjort oppmerksom på at man også i tiden før SIS kunne etterlyse folk via Interpol, så det virker som om den store utviklingen i mobilitet av folk er utslagsgivende.

9 nye medlemsland kom med i Schengen-samarbeidet i 2007; Tsjekkia, Estland, Latvia, Litauen, Ungarn, Malta, Polen, Slovenia og Slovakia (europa.eu 7.3.2013). Etter dette kan mine informanter i Kripos meddele at de har merket en stor økning i antall søk. Dette forklarer Kripos ved at mobiliteten innenfor Europa øker, flere land legger inn opplysninger, og det er generelt mer informasjon å søke på. Jeg tolker det dit hen at mine informanter i Kripos oppfatter at problemene knyttet til mobilitet har økt, men SIS bøter på og er kriminalitetsbekjempende siden det er et stort antall søk og treff.

Selv om det var ønskelig å lette mobiliteten til Europas befolkning med Schengen-samarbeidet kan det se ut til at *kriminalitetens mobilitet* man fikk med på kjøpet ikke var en direkte utilsiktet sideeffekt, men det er fristende å stille spørsmål knyttet til hvor godt det hele var gjennomtenkt. Man har riktignok kommet med en rekke kompenserende tiltak, men om politisamarbeidet og SIS klarer å holde tritt med denne utviklingen er vel heller lite trolig. En av mine informanter påpeker dette tydelig:

> *«det er vel ment at man skal kunne flytte seg omkring i Europa uten at det skal være for mye plunder og heft og byråkrati. Det blir samtidig lettere å passere grensene uten kontroll og vi ser nå resultatet av dette; det blir for enkelt å komme inn i den enkelte nasjonalstat».*

7.1.1 Tallenes tale

Jeg er klar over fellene man kan gå i når man leser kriminalstatistikk. Tallene sier ikke nødvendigvis noe om kriminalitetens forekomst, men om den kriminaliteten som blir oppdaget og anmeldt, altså den *registrerte kriminaliteten* (Høigård i Finstad og Høigård, 1997). Dette kan sammenliknes med et isfjell; det vi kjenner stikker opp, under vannflaten ligger mørketallene. Det er forskjeller med hensyn til hvor enkel kriminaliteten er å oppdage. Det er eksempelvis lettere å oppdage at noen har stjålet bilen din enn at naboen driver skattesvindel med sitt firma. Kriminalstatistikken kan heller ikke alltid leses «rett frem» i forhold til hvor det er mest kriminalitet – i noen geografiske områder og sosioøkonomiske lag kan anmeldelsestilbøyeligheten være større enn i andre. Det er også forskjeller i anmeldelsestilbøyelighet ser man på ulike typer av kriminelle handlinger (Høigård i Finstad og Høigård, 1997).

For å få et visst innblikk i kriminalitetsbildet før og etter Norge gikk inn i Schengen har jeg sett på og sammenliknet den eneste tabellen i Kriminalstatistikken som gjør en fordeling etter siktelser med statsborgerskap som variabel fra året før Norge gikk inn i Schengen; år 2000 og år 2010. Statistikken over antall siktelser kan også skjule en god del, da en og samme person som siktes for flere lovbrudd i løpet av et år kun vil bli registrert *en gang,* og registrert på det groveste lovbruddet (Høigård i Finstad og Høigård, 1997). Jeg er klar over at jeg muligens leser mye inn i tallene, for dette er «kalde» tall som naturligvis ikke sier noe om årsak-virkningsforhold. Men i lys av hvordan Schengen-samarbeidet er arrangert med hensyn til stengte yttergrenser og åpne indre grenser er det likevel interessant å se på hvordan tallene taler.

Tall fra Statistisk Sentralbyrå viser at antall siktede i Norge med utenlandsk statsborgerskap økte betraktelig i 2009 (ssb.no 10.3.2013). Dette kan til dels henge sammen med at det som vist kom nye land med i Schengen-samarbeidet i 2007. I september 2012 hadde en tredjedel av innsatte i norske fengsler utenlandsk statsborgerskap (En Helhetlig Inkluderingspolitikk, 2012). De største gruppene er personer fra Litauen, Polen og Romania (En Helhetlig Inkluderingspolitikk, 2012). Som vist kom Litauen og Polen med i Schengen-samarbeidet i 2007, og det er grunn til å anta at man nå kan se en effekt av dette. Felles for landene (inkludert Romania) er stor utreise til andre land i Europa, gjerne på grunn av arbeidsinnvandring og/eller dårlige kår i eget hjemland. Dette gjelder spesielt for Rom-folket som ønsker å søke seg til en bedre fremtid andre steder i Europa.

Ser man på Kriminalstatistikken fra år 2000, som er året før Norge kom inn i Schengen, er de overnevnte land også her langt høyere representert på siktelser til forskjell fra andre, utenom Romania som ligger lavt (Kriminalstatistikk, 2000). Polen og Litauen ligger også blant de høyeste på antall siktelser i år 2010 i tillegg til Russland og Sverige (Kriminalstatistikk, 2010). Den mest markante økningen ser vi på antall siktede fra Romania som har økt med 950 % fra år 2000 til år 2010 (Kriminalstatistikk, 2000, 2010). Det har også vært en stor økning i siktede fra Polen og Litauen med henholdsvis 188 % og 224 % (Kriminalstatistikk, 2000, 2010). Romania er som nevnt ikke medlem av Schengen, men sosiale og økonomiske vanskeligheter i hjemlandet i kombinasjon med åpne grenser i Europa gjør at mange herfra legger ut på reise. I tillegg ble forbudet mot tigging opphevet i 2005 (Lovdata, 2013), noe som har bidratt til at mange har kommet til Norge, fra Romania spesielt. Dette kan i tillegg ha ført med seg en del kriminalitet. Russland som befant seg i toppsjiktet blant siktede i år 2000 har

forholdt seg stabilt. Kriminalstatistikken sier selvsagt intet om disse personene har opphold i Norge over kortere perioder for å arbeide, men dersom det er snakk om personer som kommer seg ulovlig inn i landet og blir tatt for å drive kriminell aktivitet har styrkningen av yttergrensene i nord-områdene kanskje ikke hatt særlig effekt? Mathiesen (2013) påpeker problematikken Norge står overfor med vår lange kystgrense med tilhørende kronglete terreng. Hvordan skal vi ha mulighet til å kunne holde kontroll med denne strekningen i tilstrekkelig grad? Den utgjør en yttergrense i Schengenområdet, men oppgaven synes nesten umulig. Det kan legges til at det mest sannsynlig også vil være store forskjeller i bevoktningen av yttergrensene i resten av Schengen. Land som er preget av korrupsjon vil kunne utgjøre svake ledd i dette henseendet.

Dette bringer meg over på et noe betent, men svært aktuelt tema for Norge generelt, og Oslo spesielt. De senere årene har vi vært vitne til en stor tilstrømning av mennesker som har forsøkt å «søke lykken» i Norge, og vi har også tilstrømning av mennesker som livnærer seg av kriminalitet. Disse menneskene oppholder seg gjerne i Norge i en begrenset tidsperiode, før de begir seg videre på «Europaveien». I en aktuell artikkel fra NRK sier Politimester Hans Sverre Sjøvold i Oslo Politidistrikt at Norge er i en ekstra utsatt posisjon når vi har lave straffer samtidig som grensene er åpne (nrk.no 10.3.2013). Det lave straffenivået og det tungrodde norske systemet for å få opp en sak virker ikke preventivt. Han legger helt tydelig mye av problemet på Schengen, spesielt etter at området ble utvidet. Politiet har nå gått inn for å heve straffenivået på enkelte lovbrudds-kategorier for å bøte på problemet. I tillegg påpekes det som et faremoment at dette kan ha en stigmatiserende effekt på de fastboende innvandrerne i Norge (nrk.no 10.3.2013).

Aktuelt i denne sammenheng er at det nå har blitt åpnet opp for mulighet til å registrere tiggere i Norge ved at man har innført meldeplikt for denne gruppen (vg.no 8.4.2013). Dette vil i størst grad rette seg mot Rom-folket, og har i første omgang trådt i kraft i Tønsberg, Drammen og Bergen. Politiet vil benytte registreringen til å sjekke opp mot kriminalregistre og kan på denne måten undersøke om det er sammenheng mellom tiggerne og kriminalitet. Datatilsynet stiller seg kritisk til å gi politiet adgang til et slikt register; det strider mot personvernet, samtidig som det kan ha en stigmatiserende effekt. Tigging er heller ikke en kriminell virksomhet (vg.no 8.4.2013). Her er man inne på sammenkoblingen av data fra flere registre, og det kan være nærliggende å tro man via SIS vil benytte sjansen til å søke opp informasjon fra tiggernes fortid fra andre steder i Europa.

Det er ikke direkte enkelt å komme seg inn i et Schengenland dersom man kommer utenfra og skal over en yttergrense, slik sett har man nok oppnådd å holde sterkere kontroll med «inntrengere». Men det kan virke som man med Schengen har løftet kikkerten og sett litt for langt utover horisonten, og glemt at det er sannsynlig, om ikke *mer sannsynlig* at uønskede effekter som kriminalitet vil spres *innad i Schengenlandene* enn at den kommer langveisfra. I sammenheng med dette nevnes det fra flere av mine informanter at pass-kontrollen burde gjenopprettes.

Det å nøyaktig måle effekten av et system som SIS når man opererer i et felt som er gjennomsyret av mørketall og lukkede dører er en vanskelig oppgave. Som en av mine informanter påpeker er det gjerne slik at dersom ikke kriminaliteten synker ved overvåking, blir man gjerne møtt med at den i hvert fall stiger mindre enn den ellers ville gjort. Det er et gammelt og godt brukt argument på flere områder.

En av mine informanter føyer til:

> *«Jeg tror verken Schengen eller andre sånne konstruksjoner løser noe kriminalitet. Kriminaliteten blir mer og mer internasjonal, den blir mer og mer teknologibasert. Den evner å trekke til seg kompetanse når det gjelder å gjennomføre de lovbrudd som er under planlegging og gjennomføring».*

Som et motstykke til overnevnte utsagn kan det være grunn til å tro at fokuset ikke nødvendigvis bare bør ligge på den store «verdensomspennende organiserte» kriminaliteten som media gjerne fremstiller det som. Den største utfordringen ligger nok i «hverdagskriminaliteten» der folk som er dårlig stilt sosialt og økonomisk kjemper for egen overlevelse. Om løsningen på dette bør være registre, åpne grenser og utstrakt bruk av overvåking som en kompensasjon til et problem blant annet Schengen selv kan ha bidratt til å skape kan være vanskelig å se.

Fordelingen av fordelene og byrdene av informasjonssamarbeidet er noe ujevnt fordelt (Loader, 2002). Det vil i aller høyeste grad gå utover grupper som er sosialt og økonomisk dårlig stilt, det samme som man ser i politiarbeid på lokalt nivå. Men det som skiller politisamarbeidet i Europa er at det er rettet mot *de andre,* på vegne av *oss,* Europas innbyggere. Det retter seg i utgangspunktet mot immigranter og organiserte kriminelle som kommer utenfra. Disse blir stemplet som *fremmede, farlige* og blir gjerne værende fast i en marginalisert posisjon uten å ha mulighet til å komme seg ut av dette ståstedet (Loader, 2002). Men som vist ligger nok en del av problemet i Europa allerede.

Antakelig kan fordelene og byrdene i Schengen også være forskjellig og ujevnt fordelt rent geografisk. Det er sannsynlig at noen områder vil være mer utsatt for å «ta støyten» av de åpne grensene i Europa. Skandinavia er ikke i samme økonomiske situasjon som landene i Sør-Europa, og dette kan ha sitt å si for folkestrømmen hit.

Som Kripos påpeker bøter SIS på problemene, men til syvende og sist ser det ut til å koke ned til problematikken rundt de åpne grensene innad i Europa.
Schengen-samarbeidet vil som vist åpne opp komplekse tematiske dører til økonomiske, sosiale og politiske spørsmål.

7.2 Maktesløshet og endring i norsk rettskultur?

Lovene definerer kriminaliteten (Andreas og Nadelmann i Bowling og Sheptycki, 2012). Det vil også fra internasjonalt hold, etter hvert i større grad, bestemmes hva som skal være kriminelt i Norge.

Flere av mine informanter gir inntrykk av at vi står overfor en slags maktesløshet knyttet til det meste som foregår innenfor EU. Her nevnes vikarbyrådirektivet, post- og teledirektivet og ikke minst Datalagringsdirektivet. Det nevnes at her får man inntrykk fra myndighetenes side at det ikke er mye man kan gjøre før man kan vente seg negative sanksjoner fra EU. Det understrekes at siden nordmenn ikke har villet bøye seg for det andre land går med på blir spillerommet for oss forholdsvis lite. Dette kan igjen settes i sammenheng med Bjarne Kvams (2008) betegnelse ”cherry picking”. Norge ønsker å være med på noe, men ikke alt. Vi står overfor en overnasjonalitet; norske myndigheter er avskåret fra å treffe vedtak på områder som er overlatt til det internasjonale plan. Norge er ikke direkte folkerettslig bundet av EU organets vedtak og Norge kan ikke delta på beslutningen om nye rettsakter. Likevel har ingen EU-organ myndighet i Norge, som gjør at prinsippet om *dualisme* er ivaretatt. Dualisme kan forklares på følgende måte:

> *«Folkerettslige regler og vedtak må gjennomføres i norsk rett av norske statsorganer for å få rettslig virkning internt i Norge. Dersom det oppstår en kollisjon mellom en folkerettslig regel og det som er norsk rett, må en norsk domstol ifølge dette prinsippet gi den norske regelen forrang».* (St.prp. nr. 50 1998/99).

Norge vil uansett via kontakten med EU motta rettsregler uten at vi er med på å utforme disse. Eskeland mener Norge ved Schengenavtalen avga lovgivende myndighet fordi vi i praksis ikke kunne si nei til nye regler (Eskeland i Kvam, 2008). En av mine informanter påpeker:

> *«(…) det er et faktum at vi har ingenting vi skulle ha sagt. I den grad det kommer som direktiver så ser vi jo at vi sier jo ikke nei til dem som regel for da rakner også mye annet. Dette andre blir mer sånn bilaterale og vi kaster oss jo på det meste som faller utenfor EØS, (…) men vi kommer som sagt på grunn av det forholdet vårt ofte i en senere prosess, og da er det egentlig bare å si ja eller nei til det de andre har blitt enige om. Det er et særnorsk problem, jeg vet ikke hvor annerledes det ville blitt hvis vi hadde hatt en formell stemme, vi er jo ikke så store uansett».*

En av mine informanter nevner at når Norge i sin tid godkjente EØS-avtalen så var det nettopp reservasjonsadgangen som var bygget inn i avtalen som var et hovedargument for tilhengere for å anbefale dem som var i mot til å gå med på det allikevel.

En av mine informanter mener vi nå blir tvunget til å endre vårt syn på straff – straffeloven ekspanderer, og det er opplagt at dette vil påvirke oss i det lange løp. Vi importerer mer og mer utenifra, ikke bare popsanger, men verdier, kultur og strafferettsbekjempelse. Slik at det er ikke i og for seg noe rart at strafferettskulturen blir mer repressiv. Dette kan knyttes opp mot rettspluralisme. Det legges til at tendensen nå er at *samfunnsvernet veier tyngre enn personvernet,* og vi lar oss påvirke utenfra.

> *«(…) jeg kaller det en ond sirkel hvor det blir de som går lengst som setter standarden, fordi man argumenterer med at av respekt for de vi samarbeider med må vi ha det samme, også har du frihavn-argumentasjonen, at hvis ikke vi har det så blir vi en frihavn for rumenere eller terrorister eller hva det er. Uansett hva man mener om det så er det en veldig farlig syklus. For da blir det ikke en demokratisk og rasjonell vurdering av hva vi trenger og ikke trenger, da blir det at hvis ikke vi er like tøffe som de tøffeste så blir vi svarteper, da sitter vi igjen med alle de kriminelle i Europa. Og hvor skal det ende?»*

En av mine informanter understreker at vi har hatt en tradisjon i Norge som vi nå distanserer oss fra som har vært preget av et lavt inngrepsnivå med lave straffer, lite inngripende metoder i etterforskning og lite inngripende muligheter for å overvåke mennesker. Det norske systemet var for inntil en 10-12 år siden preget av en ”jomfruelig uskyld”. Det legges til at dette handler om globalisering, ikke bare en økonomisk globalisering, men også en kulturell globalisering når det gjelder vår oppfattelse av kriminalitet. Kriminaliteten globaliseres og blir transnasjonal. Muligens går vi i retning av et hardere klima kriminalitetsmessig, og andelen utenlandske fanger i Norge er stor. Hele rettskulturen endres som følge av globalisering. Et eksempel som nevnes er at vi har hatt straffebestemmelser som har vært basert på det

hovedprinsipp at forberedelser til straffbare handlinger har vært straffrie - man har kunnet ombestemme seg. Som nevnt tidligere kan man registreres i SIS om det foreligger mistanke om at man planlegger en kriminell handling.

> *«Det som skjer for Norges del er at Norge mister sin… tak i sin egen tradisjon… for det som styrer et sånt internasjonalt samarbeid det er jo en mer repressiv rettskultur enn hva vi har vært vant til. Og det er de mest repressive rettskulturene som virker mest dynamiske i sånne samarbeidsforhold. Så derfor vil dette altså påvirke Norge i retning av mer overvåking og en mer repressiv rettskultur».*

Selv om Norge er medlem av Schengen står vi som land likevel mye utenfor politisamarbeidet (Kvam, 2008). Norge er ikke deltakende på så mye av det som gjelder for Schengen og utviklingen av avtalen annet enn for SIS. Kvam mener Schengens deltakelse bærer preg av avvikling snarere enn videreutvikling. Dette kan skyldes at mye av strafferettssamarbeidet og politisamarbeidet er tett vevet ved andre sider av EU som Norge ikke tar del i. Norge beskyldes litt for å «skumme fløten» i den forstand at Norge kun delvis ønsker å involvere seg, men gjerne vil høste fruktene. Synet blir da fra en del land i Europa at Norge får ta til takke med det de får.

Norge vil ta del i det europeiske reisefrihetsområdet, som også er det egentlige eksistensgrunnlaget for hele avtalen, men i følge Kvam er politi – og strafferettssamarbeidet i ferd med å bli faset ut (Kvam, 2008). Om denne antakelsen stemmer kan selvsagt diskuteres. SIS II har blitt lansert og Norge vil også benytte dette systemet. Kanskje vil samarbeidet utvikle seg i enda større grad? Kvam skriver at for Norges del var Schengen-samarbeidet eneste mulighet for å bevare passfriheten mellom de nordiske landene, og med på kjøpet fikk vi et begrenset politi – og strafferettssamarbeid med EU.

Tendensen er nå tilsynelatende at Norge ønsker sterkt å være med, men holdes i stor grad utenfor (Kvam, 2008). Om dette er unaturlig kan selvsagt diskuteres. Vi ønsker å være med på det som kan virke positivt i vår favør, men vil ikke være medlem av EU. ”Utenforskapet” på sin side vil føre til at Norge ikke trenger å innrette seg etter straffelovgivningen som bestemmes fra Brussel. I rådsbeslutningen av 17.mai 1999 er det sagt at Norge alltid skal delta i videreutviklingen av SIS. Har Norge her forsøkt å sikre seg? Norge kan ikke være med på å videreutvikle 23 av de 57 reglene rundt politi og strafferettssamarbeidet. Disse reglene har en mer ”markert EU-identitet” som gjør at Norge ikke får delta (Kvam, 2008).

Man skal selvsagt ikke glemme det man forsøker å oppnå ved overvåking. Politisamarbeidet har som mål å øke sikkerheten i Europa, men det krever en viss balanse mellom målet og de konkurrerende mål og verdier (Loader, 2002). Er det slik at man må gi avkall på grunnleggende menneskerettigheter og verdier for å oppnå ønsket grad av sikkerhet? Politiet vil operere på et felt med eksempelvis transnasjonal kriminalitet i hovedfokus som vil være fjernt fra en vanlig borgers liv. (Loader, 2002). På bakgrunn av dette kan en Schengen-innbygger ha andre verdier enn de som opererer på toppen av det hele. Det er en liten mektig gruppe som styrer politisamarbeidet fremover, og deres krav og fremmedfrykt speiler ikke nødvendigvis den demokratiske stemme i Europa (Loader, 2002). Siden det hele kan fremstå som veldig fjernt fra oss, og sannsynligvis også noe fjernt fra de fleste politifolks hverdag kan det være en løsning å inkludere de lokale politiorgan i større grad. Håpet er at dette skal kunne bidra til å legitimere arbeidet i Europa i større grad (Loader, 2002).

Walker benytter begrepet «national sovereignty trap» til å beskrive prosessen der nasjoner enten vil kjempe for å få makten tilbake til egen stat, eller at man forsøker å få enda mer utnytte av det som avgjøres fra EU-hold (Walker i Loader, 2002). Storbritannia er et eksempel på dette der man forsøker å holde tilbake, for ikke å gjøre om på den Europeiske integrasjonen (Loader, 2002). Samlet sett er det sikkerheten i Europa som opptar de offentlige myndigheter, målet er ikke å bevare demokratiet i Europa (Loader, 2002).

8 Europaveien videre – hva nå?

Selv med mange systemer og samarbeid i gang er ennå flere i startgropen og på tegnebrettet. Med Schengen-samarbeidet var det en målsetting at Schengens borgere skulle kunne reise enkelt innad i landene uten papirmøller og byråkrati som reisefølge. Nå ser man i større utstrekning på muligheten for også å lette krysningen av EU's yttergrenser, spesielt ment for å lette reisen til de som reiser mye. Overvåkingen generelt øker som følge av dette. Hvor går veien videre?

8.1 Et panoptisk liv?

Lite tyder på at utviklingen knyttet til overvåking kommer til å snu. Samtlige av mine informanter er overbevist om at utviklingen bare vil fortsette i retning av mer overvåking og kontroll.

Som en av mine informanter beskrev det:

> *«Ja, det kommer til å bli mer av det. Jeg tror at våre liv kommer til å bli totalt gjennomsiktige. De skal ha tak i våre fingeravtrykk og DNA og alt mellom himmel og jord. De skal ha gjøren og laden – Datalagringsdirektivet er jo gjøren og laden. Det er bra at det er noen kriminelle som er så utkrøpne at de klarer å overliste disse systemene, for alternativet er så utrolig skummelt. Hvis ingen klarer å overliste et system… hvis alt skal være helt gjennomsiktig… Hva er det Nils[9]sier; en passende mengde kriminalitet? Alt som tar sikte på å skape idyll på jorden vil ende opp med å gjøre det til et helvete».*

Min informant understreker at det er overvåkingens og kontrollens skjulte karakter som er problematisk.

> *«Jeg vil foretrekke å bli grundig eksaminert på Svinesund fremfor ikke å bli eksaminert i det hele tatt, men å vite at jeg blir overvåket innenfor de nasjonale grenser med tanke på fra myndighetenes side for å finne ut hva jeg driver med, hvor jeg driver med det, om det er lovlig, om det er i overensstemmelse med norsk lov, om jeg har kommet lovlig inn i EU-området, innenfor Schengen-området osv... Jeg liker den form for overvåking som knytter seg til en mann som har på seg konstabeluniform (…)».*

Det er trolig at behovet for å holde øye med borgerne innenfor et definert geografisk område vil øke.

[9] Henviser til Professor i kriminologi Nils Christie.

Det at man blir utsatt for overvåking i så stor grad kan muligens føre til at man vil endre sin atferd på bakgrunn av dette. Dette blir en slags vekselvirkning – man tilpasser seg til kontrollmetodene, og overvåkingen kan slik muligens speiles i kriminaliteten.

Det er mange elektroniske spor etter oss i samfunnet og min informant mener vi får en større bevissthet med å kunne opptre relativt sporfritt, selv om det er vanskelig. Min tanke er at dette kanskje følger hverandre; ved at overvåking og registrering foregår i det skjulte vil dette kanskje føre til at folk vil opptre på en mindre synlig måte enn tidligere. Kanskje vil man tilpasse sin atferd til måten man vil bli fulgt på. Samtidig som samfunnet med de høyteknologiske nyvinninger blir mer og mer gjennomsiktig, så kan det muligens tenkes at kriminaliteten i større grad blir mer og mer skjult fordi den evner å tilpasse seg dette.

8.2 Smartborders

Min informant fra EDPS gjør meg oppmerksom på planene knyttet til såkalte «Smartborders». Det gikk ut pressemelding fra Europakommisjonen i 2011 om at dette var en av de fremtidige planene, og det er nå på prøvingsstadiet.

Man ser i dag en økning i antall flypassasjerer i EU, og det er beregnet at i 2030 vil antallet passasjerer ha steget med 80 % sammenliknet med tall fra 2011 (European Commission, 2011). For å kunne imøtekomme behovet og unngå køer på flyplassene implementeres «Smartborder-konseptet». Man skal lette reisen til de som reiser mye inn og ut av EU-området samtidig som man vil heve overvåkingen ytterligere ved ankomst/utreise og registrere data om lengde på opphold og liknende (European Commission, 2011).

Dette blir som en virtuell grense der tredjelands borgere vil bli registrert elektronisk. Man finner dette eksempelvis mellom USA og Canada. Det er også et annet forslag ute om å etablere et program for de som reiser mye der disse for eksempel har en token i stedet for pass. Dette er også relatert til Smartborder-konseptet.

Smartborder-konseptet har allerede blitt implementert i noen land i Europa. Min informant i EDPS nevner flyplassen Schiphol i Nederland der man har en gate man kan passere uten å bli kontrollert av grensevakt.

Smartborder-konseptet vil nok også bli en brikke i det internasjonale samarbeidet som vil føre til at utvekslingen av informasjon forsterkes, og vil sige ut av Europa til samarbeidende myndigheter.

Det kan påpekes som noe merkverdig at man nå sjekkes for alle mulige tingester, flytende væsker og skarpe gjenstander, mens det ikke er så farlig med passet. Det er noe med ordningen som ikke henger helt på greip.

8.3 Mulige Scenarier – Schengenveien videre

Som jeg forhåpentligvis har klart å vise leseren, er politisamarbeidet i Schengen involvert i en kompleks masse av temaer knyttet til rettssikkerhet, kriminalitet, personvern, teknologi og menneskerettigheter som igjen reiser en uendelig rekke spørsmål.

Jeg vil her avslutningsvis skissere og diskutere et par mulige scenarier for Norges del med hensyn til Schengenveien videre. Dette vil hovedsakelig basere seg på mange av mine egne betraktninger jeg har gjort meg underveis i arbeidet. Jeg vil også vise at sammenhengen mellom rett og samfunn utkrystalliseres i et slags symbiotisk forhold, der man kan søke å endre retten eller rettsstrukturer for å endre en tendens i samfunnet.

8.3.1 Scenario 1: Norge går ut av Schengen

En mulighet for Norges del er å trekke seg fra medlemskapet i Schengen. Jeg ønsker her å diskutere konsekvensene av dette og hvorfor det er en mulighet.

Konsekvenser av utmelding

Dersom Norge går ut av Schengen vil dette bety at vi ikke lengre vil samarbeide med politiet i andre Schengenland via SIS vi nå har blitt vant til å benytte, og dette kan til dels amputere vår evne til å være deltakende og ovenpå i etterforskningen av grenseoverskridende kriminalitet. Kanskje kan vi likevel delta i en del av de andre systemene som er nevnt tidligere. Vi vil i et slikt tilfelle også måtte bygge opp igjen grensekontrollen på Norges yttergrenser, og vårt

ønske om å sette i stand igjen *Det Nordiske Reisefrihetsområdet* kan fort melde seg. Om dette vil være enkelt å få i stand vil ikke være så sikkert. Schengens yttergrense vil da ligge mot Norge, og de land som grenser mot oss vil være bundet opp av sin plikt til å holde en streng grensekontroll til land utenfor Schengen. Dette kan føre til at man må medbringe pass dersom man ønsker å avlegge et lite besøk på Svinesund.

Vi vil med dette ikke samarbeide med de 25 gjenstående landene via «stjernedrysset» av systemer i den grad vi gjør i dag, og vil på denne måten bli satt på utsiden i større grad enn vi allerede er med vårt «utenforskap» i EU. Vi vil muligens slippe å få en «strøm» av mennesker over grensene i tilsvarende grad som vi ser konturene av i dag, da grensene bevoktes av oss selv. Om vi vil klare å opprettholde en sterk grensekontroll ut i fra hvordan reisetrenden til Skandinavia er i dag er selvsagt uviss. Det kan være fristende å la tankene vandre til skjærgården mellom Norge og Sverige – mon tro om dette kan være en enkel vei inn i landet? Lite tyder på at Norge skulle skille seg fra andre land der sjøveiene ofte er mye brukt både med tanke på trafficking og smugling.

Senterpartiungdommens rolle

Etter mange år i dvale har den politiske debatten rundt Schengen i 2013 så smått blitt blåst nytt liv i, og spørsmål knyttet til Norges medlemskap har blitt reist flere ganger i mediebildet. Schengen-samarbeidet blir gjerne utpekt som syndebukk for de synlige effekter man kan se spesielt i Oslos gatebilde. Dette ser ut til å være en tematikk som folk engasjerer seg i, og dette er kanskje medvirkende til at mediebildet omtaler dette i overraskende stor grad i skrivende stund? Norges borgere, spesielt i byene, kan etter hvert begynne å identifisere seg med denne problematikken. Schengen er ikke lenger bare «ett eller annet fra Brussel som har med pass å gjøre», men personer som sitter med pappkruset holdt opp og som ser med sorgtunge øyne på en når man passerer. I mange reises både sympati og raseri. Politiet ser sammenheng mellom tiggerne og kriminalitet.

Senterparti-ungdommen har tydelig flagget sitt ønske om å komme Schengen til livs fordi de mener det er en klar sammenheng mellom flere utenlandske kriminelle og passfriheten til Norge (Melgård, 2013). Men som utenriksminister Espen Barth Eide kommenterer: «*Jeg vil minne om at grensekontroll ikke begrenser tilgangen for kriminelle. Det står ikke «bankraner» i noens pass, det er ingen som oppgir i en grensekontroll at de kommer til landet for å stjele og rane*». (Eide i Melgård, 2013). Denne kommentaren er selvsagt korrekt, men

det er en forskjell på helt åpne grenser der man overhodet ikke vil følge med på hvem som kommer inn og ikke sitte med noe kontroll, enn så langt det lar seg gjøre ha oversikt over hvem som befinner seg i landet. Men man kan aldri sikre seg helt mot falske dokumenter og pass, samtidig som noen alltids vil finne andre veier inn i landet. Slik situasjonen er i dag kan man i busslaster om så ønskelig er passere Svinesund uten at noen legger seg opp i dette. Den gylne middelvei, eller «grensevei» om man vil, finner man i hvert fall ikke med Schengen-samarbeidet. Men man skal også være klar over det faktum at alvorlig kriminalitet som trafficking og narkotikasmugling spres hurtig i land, langt utenfor Europa, der bevoktningen av grensene er streng. Det er ikke dermed noen garantier for at dersom man gjenopptar grensekontrollen vil dette kunne ha de klare effekter man ønsker. Kriminalitet som smugling, trafficking og liknende blir imidlertid i større grad beheftet med risiko dersom man gjenopptar grensekontrollen, og dette kan muligens ha en noe preventiv effekt. Dette er ikke bare å skru av en bryter; vi har folk som oppholder seg i Norge, mange av disse er vi ikke klar over i det hele tatt. Men trolig vil en utmelding av Schengen kunne være et steg på veien i å oppnå de ønskede mål.

Global kriminalitet og kriminalitet i norsk bybilde

Det kan være viktig at man holder et skille mellom den «*globale, verdensomspennende, organiserte kriminaliteten*», og overnevnte personer vi finner i bybildet i Norge der mange kjemper for egen overlevelse. Dette er et meget komplekst problem, ikke minst på bakgrunn av Rom-folkets sosiale situasjon og ståsted som har røtter svært langt tilbake i historien, lenge før Schengen var på tegnebrettet. Disse personene har ikke startet sin reise med Schengen som drivstoff, men har vært «jaget» av ulike årsaker fra landområder gjennom hele deres historie. Det kan ikke her gås i dybden av denne problematikken, men slik mediebildet former seg i disse dager ser det ut til at det hovedsakelig er denne gruppen man er ute etter. Som nevnt tidligere er ikke Romania medlem av Schengen, men av EØS. Borgere fra EU/EØS/EFTA-land har rett til å besøke Norge uten oppholdstillatelse, og dette vil ikke endres dersom Norge går ut av Schengen. Forbudet mot tigging som ble opphevet i 2005, (Lovdata, 2013) med ikrafttredelse juli 2006 kan ha hatt sitt å si – forbudet ble altså hevet 5 år etter at Norge gikk inn i Schengen og man har sett en markant økning av personer fra Romania etter dette. Det å innføre forbudet mot tigging kunne vært et aktuelt tiltak i første omgang uten at dette vil få så vidtrekkende konsekvenser som det å gå ut av Schengen. Går man til kjernen av problemet ser det ut til at man hovedsakelig forsøker å få bukt med Rom-

folket, og spesielt de som i tillegg bedriver kriminell aktivitet. Går man for dette alternativet er ulempen at man vil slå alle over en kam, også de som *kun tigger*, og tiggere med *norsk statsborgerskap*. Dette vil heller ikke løse problemet som bunner i Rom-folkets fattigdom og nød, men et tiltak som kan bære preg av desperasjon fra norske myndigheter. Det vil også kreve kapasitet fra politiet for å håndheve dette. Det er legitimt å stille spørsmålet om dette løsningsforslaget kan bringe med seg en uønsket sideeffekt som eksempelvis mer kriminalitet blant tiggere.

For lettvint å legge skylden på Schengen?

Kanskje er det for lettvint og noe forhastet å legge hele byrden og «skylden» på Schengen-samarbeidet. Norge er tett vevet sammen med Europa på andre arenaer, ikke minst via EØS. Selv om tallene som nevnt tidligere taler i retning av at Schengen er en medvirkende faktor i den utviklingen vi ser i dag, står heller ikke Schengen helt alene om dette. EØS representerer med sine *fire friheter* rettigheter for EØS-landene som skal sikre fri flyt av tjenester, varer, kapital og *personer* (Agreement on the European Economic Area, 2011). EØS er også mer omfattende i sitt omfang med 30 medlemsstater. Når avtalen gir rett til fri flyt av personer, fortrinnsvis med tanke på ansettelse i et EØS-land (Agreement on the European Economic Area, 2011), vil dette kunne gi personer rett til å ferdes fritt i EØS selv uten Schengen på banen. Riktignok er ikke Rom-folket kommet til Norge for å søke arbeide, men så er det vel heller ingen som har tilbudt denne gruppen arbeid?
EØS-avtalen er svært omfattende og setter sitt avtrykk både i næringsliv og norsk politikk, ikke bare ved muligheten den gir personer for å ta arbeid i et annet EØS-land. Norge er med dette ikke lenger et isolert land i nord, men på flere områder knyttet tett opp mot resten av Europa. Totalt sett er dette et meget komplisert felt, og vurderingen av dette og veien videre er ikke enkel. Både EØS og Schengen har også effekter som er positive for Norge, og ved en eventuell utmelding må vi også være forberedt på at vi vil sitte igjen uten en del rettigheter andre land i Europa vil ha. Slik sett er det ikke noen garantier for at man vil oppnå de ønskede og tilsiktede effekter ved å melde Norge ut av Schengen.

Signal til Europa

Dersom vi melder oss ut vil vi kanskje også sende et uheldig signal ut i Europa? Vi vil muligens ytre et generelt ønske om distansering og vi vil fraskrive oss de menneskene som av

sosiale årsaker er på jakt etter en bedre fremtid. Vi vil vende ryggen til det meste av problemer samarbeidet har ført med seg samtidig som vi plasserer alt av ansvar på de gjenværende Schengenlandene. Vi vil heller ikke kunne få hjelp og informasjon fra de tidligere samarbeidende myndigheter i Schengenområdet som vi var en del av.

Norge har vært medlem av Schengen-samarbeidet i 12 år i skrivende stund – og vi har blitt både negativt og positivt berørt av samarbeidet. De problemene som har dukket opp i vårt land vil vi muligens stå alene om å løse. Personopplysninger vil ikke lenger strømme ut fra Norge via SIS, men hva med alle opplysningene som allerede er på «vidvanke»? Vi kan igjen se til Apenes og angre på at vi var ivrige til å «konservere høystakker» av informasjon.

Vi vil også måtte huske passet når vi skal ut og reise til et av de 25 gjenværende Schengen-landene, mens deres borgere kan reise enkelt rundt i Europa. Antakelig kan dette oppfattes som urettferdig av mange. Hvorfor skal en norsk borger kontrolleres grundigere ved en grense enn en borger fra Spania? At Norge blir en «outsider» i ganske stor grad er det liten tvil om, men man må her gjøre en vekting av fordeler og ulemper. Vi har nå blitt tett vevet inn i resten av Europa både politisk og økonomisk; kanskje er det for sent å trekke seg nå?

8.3.2 Scenario 2: Et kombinerende tiltak

Som vist kan åpne grenser innad i Schengenområdet være en bidragende årsak til mobilitet av personer som gjør at også kriminaliteten og mennesker i sosial nød flytter på seg. Norge er i en posisjon til å kunne ta seg av en del mennesker som lider, mens mange andre land i Europa ikke har denne evnen. For Norges del later det kanskje til å være et spørsmål om vilje, ikke om evne? Kanskje er vi også raske til å sette merkelapper med «kriminalitet» på steder der det ikke hører hjemme, som også har vært en fare med Schengen og SIS.

Man kan stille spørsmålet; hvor viktig er det for den gjengse europeer å kunne reise til et annet Europeisk land uten å måtte ta med seg passet? Er reisefriheten laget av og for eliten som er hyppig på reisefot? Likevel er det å skulle medbringe et pass en smal sak, også bokstavelig talt. Med dagens økonomiske situasjon i en del land i Europa er kanskje heller ikke reiseliv høyest oppe på agendaen?

Informasjonssamarbeidets irrganger skjuler som vist mange problemer knyttet til individers rettssikkerhet og personvern. Likevel har det den gevinsten at man kan samarbeide med politimyndigheter i andre land og vil kunne være et verdifullt instrument i etterforskning. Man vil også på denne måten kunne holde større kontroll med personer ved bruk av informasjonssystemene. Samtidig har vi bygget opp en «mur» mot utsiden av Europa.

I pose og sekk

Kan man tenke seg en kombinasjon av at man beholder en del av politisamarbeidet, men samtidig har strengere grensekontroll slik situasjonen var før Schengen-avtalen? Dette vil i hvert fall kunne føre til at Schengen-samarbeidet i høyere grad kan konsentreres om de problemer som kommer via kryssing av grenser fra tredjeland som var dets formål i utgangspunktet, og ikke i så stor grad sentreres rundt de problemer den later til selv å ha bidratt til å skape. Dette kan virke som mye å be om, men ut fra opplysningene fra Statewatch er England et eksempel på at dette er mulig der man selv har ansvaret for egne grenser, men samtidig har tilgang til SIS. Situasjonen for England vil likevel være noe annerledes da England ligger på et øyområde og skiller seg slik klart fra alle andre land i Europa. På den annen side er vi medlem av EØS, så dersom vi virkelig ønsker «å skalke lukene» vil vi måtte melde oss ut av denne avtalen i tillegg.

Statsvakt

Beholder man politisamarbeidet i overnevnte løsningsforslag får man fortsatt med «katta i sekken» i form av problemene jeg tidligere har skissert med hensyn til personvern og rettssikkerhet. Her er fremdeles veien lang å gå, om ikke lengre enn tidligere. I tillegg til de tiltak som allerede er nevnt kan man gå videre med et forslag som igjen løfter viktigheten av de ikke-statlige organisasjonene inn på banen. Mathiesen (2000) bidrar med et forslag som står like aktuelt i dag – 13 år etter, som igjen bringer oss til de ikke-statlige organisasjoner. Med hans «Statsvakt» som vil minne mye om den engelske organisasjonen «Statewatch» vil man kunne ha en liten organisasjon som på heltid vies til å følge med på det som foregår i EU. Ikke minst vil vernet av individers rettssikkerhet og personvern også måtte gås etter i sømmene. Skal man bli værende i politiarbeidet må man ha en organisasjon som ikke har noen egeninteresser eller staten som brensel. Dette er noe man bør vurdere om dette scenariet utspilles. Men spørsmålet er selvsagt om hjelpen fra dette vil monne mot et så enormt

maskineri som politisamarbeidet med alle dets systemer representerer, i likhet med de problemer dagens NGO's møter.

Scenariet som har utspillet seg med SIS kan sammenliknes med historie generelt; vi kan ikke endre den, men vi kan se tilbake på den for å unngå å begå de samme feil i fremtiden. Etterpåklokskapen i SIS' henseende er ikke mye til hjelp dersom man ikke er føre var og bygger opp systemene med tanke på personvern og rettssikkerhet i utgangspunktet. Forsøker man å gjøre dette senere blir operasjonen for stor, kostbar og uhåndterlig.

SIS II har i skrivende stund blitt lansert for to dager siden. Det gjenstår å se om de regelverk som knytter seg til det nye systemet er utbedret og om man ved en ny kontrollør på banen i form av EDPS vil få mer orden i «SIS-sakene». Vi må finne en måte å leve med systemene. De er kommet for å bli.

8.4 Videre forskning

Det å skulle kartlegge et så omfattende terreng som Schengen-samarbeidet faktisk utgjør er ikke en enkel oppgave. 26 land inngår i samarbeidet og det er mange variabler som krever utredning. Jeg har tatt for meg rettssikkerhet, personvern og sett på effekten av Schengen-samarbeidet i de store trekk.

Det har vært gjort forskning innen EU, et eksempel her er det treårige forskningsprogrammet *Detecter* som ble gjennomført med Universitetet i Birmingham som koordinator fra 2008-2011 (detecter.eu 28.3.2013). Programmet tok for seg bekjempelse av terrorisme, databruk i etterforskning og menneskerettigheter (detecter.eu 28.3.2013). Et annet og mer Schengenrelevant eksempel er forskningsprosjektet *INEX* som under ledelse av norske PRIO studerte utviklingen i Europa med mer og mer utflytende grenser, teknologi og transnasjonale sikkerhetsforanstaltninger (inexproject.eu 28.3.2013). Prosjektet holdt seg imidlertid ikke tematisk kun til Europa (inexproject.eu 28.3.2013).

Det er likevel mangel på forskning som går direkte på Schengen og dens effekter. Om man virkelig skal trenge inn i materien vil man måtte gå til verks i et omfang som for lengst vil sprenge de tidsmessige og ikke minst økonomiske grensene for en masteravhandling. Dessuten vil man måtte trenge gjennom murer som bærer preg av de sterkeste former for

sikkerhetsklarering, så en kan ikke forske fritt innenfor den tematiske grensen til Schengen uten videre. Jeg ønsker her å skissere et par mulige veier å gå med tanke på forskningen videre.

8.4.1 Kommisjonsarbeid

De store kontrollørene som ser til at Schengen samarbeidet fungerer etter gitte retningslinjer og rapporterer videre i EU, som JSA og EDPS, vil utføre sitt arbeid med EU i ryggen. Man kan tenke seg at dette vil kunne farge deres syn og tilnærmingsmåte. Man har i tillegg til dette planlagt kommisjonsarbeid, der man avlegger besøk i Schengen-medlemsstatene både varslet og uvarslet (europa.eu 2011, 28.3.2013). I denne sammenheng har man også planlagt å sette i gang en «Schengen Health Check» to ganger i året der man tar «pulsen» på Schengen og gjør en vurdering av situasjonen (europa.eu 2011, 28.3.2013).

Disse tiltakene er selvsagt vel og bra, men jeg har likevel et forslag til noe jeg ser på som en forbedring. En mulighet er å engasjere helt *utenforstående aktører*, enten private eller fra ikke-europeiske land. Dette vil måtte være et team profesjonelle med spisskompetanse både innen IT, personvern og jus. De vil måtte gis mandat og økonomiske ressurser til å komme på innsiden av systemet og forske fritt og uforstyrret. Disse vil måtte engasjeres over lengre tid og avlegge samtlige Schengenland besøk for å kunne kartlegge hvordan arbeidet utføres og påpeke forbedringstiltak. Ved at de besøker alle land vil man kunne få et nøytralt helhetlig bilde som kan fremstilles i en omfattende rapport som overleveres. Slik overvåkningen av arbeidet i dag fremstår er den noe oppstykket da JSA har kandidater som byttes ut, og EDPS ikke går systematisk til verks i så måte.

Bakdelen ved dette vil være at man må gi «uvedkomne» innsyn i den delen av Schengen samarbeidet som er mest hemmeligholdt. Og man må selvsagt sikre i størst mulig grad at dette ikke vil sette personvernet i fare. Men her vil muligens målet måtte hellige middelet, og jeg er nokså sikker på at det ville være verdt det.

8.4.2 Statistiske analyser

Det er interessant og ikke minst svært nyttig å studere kriminalitetsutviklingen etter at de fleste europeiske land gikk inn i Schengen-samarbeidet. Om det er en reell bieffekt av Schengen at kriminalitetens mobilitet har økt innad i Europa slik det ser ut til bør studeres nærmere og mer systematisk.

For å få innblikk i kriminalitetsutviklingen i de ulike landene bør man studere den nasjonale kriminalstatistikken i alle 26 medlemsland. Uten at jeg har hatt mulighet til å sette meg inn i dette kan det muligens være forskjeller landene i mellom med hensyn til hvordan denne føres, og hvor nøyaktig den oppdateres. Med dette in mente bør man uansett se nærmere på dette for å kunne fastslå om Schengen har gitt oss en del effekter vi helst kunne vært for uten. Dette arbeidet kunne blitt utført av overnevnte kommisjon.

Som jeg nevnte i metodekapittelet ville det vært interessant å studere befolkningens kjennskap til Schengen og hva dette innebærer ved en kvantitativ undersøkelse. Mitt forslag er at denne burde gjøres i samtlige land og per telefon. Mest sannsynlig ville en telefonundersøkelse gitt størst representativitet da de fleste er eier av en telefon, selvsagt med visse forskjeller landene i mellom. Dette kunne gitt en interessant indikasjon på hvor kjent eller ukjent politisamarbeidet og dets effekter for folks personvern og rettssikkerhet er.

Skal man kunne gjøre de riktige beslutninger i fremtiden med hensyn til Europaveien videre ser jeg det som avgjørende at man gjør en utførlig kartlegging av situasjonen slik den fremstår i dag. Arbeidet jeg har skissert er ikke lite, men jeg mener langt på vei at det er verdt det.

9 Konklusjon

Veien ser ut til å være lang og gå, om ikke lengre enn noen gang med tanke på rettssikkerhet og personvern i SIS. Nå når SIS II har blitt lansert med et ennå mer komplekst datainnhold vil spørsmålene knyttet til de nevnte utfordringer tilta. Det er en vanskelig balansegang, for samtidig som politiet i økende grad er avhengig av å samarbeide på internasjonalt nivå ser de farer som informasjonssystemene fører med seg ut til å ekspandere. Det er det totale overvåkingsbildet som kan sies å være den største faren.

Datatilsynet og andre EU-kontrollører er på banen, regelverk skrives og distribueres. Man har disse viktige tingene in mente, og det nevnes utførlig i Schengenkonvensjonen. Men det ser likevel ikke ut til at dette er tilstrekkelig. Det går et tydelig skille mellom det som skrives på papiret og hvordan det fungerer i praksis. Schengen-samarbeidet legger opp til at utøvelsen av samarbeidet kan være ulik i de forskjellige medlemslandene. Det å tilstrebe likhet i alle land vil i hvert fall være et sted å begynne. Dersom situasjonen er slik at opplysninger er i større fare i noen medlemsland enn i andre er dette noe som må kartlegges og tas tak i.

Kompleksiteten av informasjonssamarbeidet øker i omfang. Selv om SIS ser ut til å spille hovedrollen i kontrollmaskineriet kommer stadig nye systemer til som vil kunne flytte og benytte bruddstykker av informasjon som gjør at kontrollblikkene ikke klarer å henge med. Man vil drukne i informasjonsstrømmen man forsøker å holde kontroll på. Databasene og systemene innad i Europa blir et finmasket nett, informasjonen kommer antakelig i større grad til å flyte ut av Europa og kontrollen blir ennå vanskeligere å opprettholde enn den allerede er. For kontrollerende myndigheter som Datatilsynet å skulle holde kontroll på detaljnivå synes som en umulig oppgave man av kapasitetsmessige hensyn ikke har mulighet til å imøtekomme. For de ikke-statlige organisasjoner som engasjerer seg i dette vil oppgaven også være vanskelig, og man kan kun følge med på et overordnet nivå.

På denne måten er hovedansvaret lagt på utøverne av systemet selv, som i den daglige driften vil være den viktigste kontrolløren av eget arbeid. Vi står overfor et skifte i kontrollen av SIS ved at EDPS vil ta over hovedansvaret for kontrollen. Om dette kommer til å forbedre situasjonen gjenstår å se.

Som vist har Schengen-samarbeidet tilsynelatende dratt med seg en del sideeffekter, og man har forsøkt å kompensere for dette med utstrakt bruk av politisamarbeid. Så lenge grensene

innad i Schengen er åpne vil nok ikke de problemene vi ser i dag avta. Men som jeg har vist står ikke Schengen alene som problemskaper; vi har også EØS og lokale særegenheter som gjør at dette problemet ikke med enkelhet lar seg løse.

Man kan stille seg spørsmålet om et informasjonssystem vil kunne klare å kjempe mot disse krefter, selv om det øker i kompleksitet. Kanskje burde vi igjen ha grensekontroll, og ta med oss passet i baklommen når vi legger ut på Europaveien. Det er et sted å begynne.

På bakgrunn av det jeg har vist og de farer Schengen-samarbeidet produserer både med hensyn til rettssikkerhet, personvern og statssikkerhet generelt er det noe utfordrende å meisle ut særs gode argumenter for opprettholdelsen av Schengen-samarbeidet sett i sammenheng med dets målsettinger. Jeg stiller meg tvilende til retningen utviklingen ser ut til å ha tatt og hvordan utviklingen vil gå fremover. Slik situasjonen er i dag kan det se ut til at tapet totalt sett er større enn gevinsten.

Litteraturliste

Agreement on The European Economic Area (2011). (OJ No L 1, 3.1.1994, p. 3; and EFTA States' official gazettes) 15.11.2011 (updated) Brussels.

Apenes, Georg (2000): *Panoptikon. Vårt gjennomsiktige samfunn*. Oslo: Geelmuyden Kiese.

Apenes, Georg (2010): *Skal storebror vite alt om deg?* URL: http://tb.no/arkiv/skal-storebror-vite-alt-om-deg-1.1136314 TB.no Tønsberg blad. (13.1.2010). [Lesedato:7.1.2013].

Beck, Ulrich (1986): *Risksamhället. På väg mot en annan modernitet.* Suhrkamp Verlag.

Boehm, Franziska (2009): "Confusing fundamental rights protection in Europe: Loopholes in Europes fundamental rights protection exemplified on European data protection rules". I: *Law Working Paper Series. Paper number 2009-01*. Faculty of Law, Economics and Finance, University of Luxembourg.

Bowling, Ben (2009): "Transnational Policing: The Globalization Thesis, a Typology and a Research Agenda". I: *Policing, Volume 3, Nr. 2*. S.149-160. Oxford University Press.

Bowling, Ben og Sheptycki, James (2012): *Global Policing.* London: Sage Publications Ltd.

Brouwer, Evelin (2008): *The Other Side of Moon. The Schengen Information System and Human Rights: A Task for National Courts.* CEPS Working Document No.288/April 2008.

Bunyan, Tony (1993): "Trevi, Europol and the European State". I: *Statewatching the new Europe*, 1993/14.

Bunyan, Tony (2006): *The "principle of availability".* Statewatch.

Calabrese, Leonardo (2011): *The Rule of Law Reform Process in Bulgaria and Romania.* URL: http://csis.org/blog/rule-law-reform-process-bulgaria-and-romania [Lesedato:17.3.2013].

Council of the European Union (1999): "Council Decision of 20 May 1999". I: *Official Journal of The European Communities.* 10.7.1999.

Council of the European Union (2005): *Prüm Convention.* Council Secretariat.

Council of the European Union (2013): *Schengen information system database statistics 01/01/2013 7389/13.* Brussels.

Dalberg-Larsen, Jørgen (1994): *Rettens enhed – en illusion?* København: Akademisk Forlag.

Datatilsynet.no (2011a): *Hva er personvern?*
URL:http://www.datatilsynet.no/personvern/Hva-er-personvern/ [Lesedato:18.2.2013].

Datatilsynet.no (2011b): *Personvernprinsippene*.
URL:http://www.datatilsynet.no/personvern/Personvernprinsipper/ [Lesedato:19.2.2013].

Datatilsynet (2012): *Endelig Kontrollrapport 2012*.

Detecter.eu (2013): *Detection Technologies, Terrorism, Ethics, and Human Rights*.
URL: http://www.detecter.eu/index.php [Lesedato: 28.3.2013].

Edps.europa.eu (2013a): *Duties.*
URL:http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Membersmission/Duties [Lesedato: 5.2.2013].

Edps.europa.eu (2013b): *Joint Supervisory Authorities.*
URL:http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/79 [Lesedato:6.3.2013].

Endringslov til SIS-loven. *Lov om endringer i lov 16. Juli 1999 nr. 66 om Schengen informasjonssystem (SIS).* LOV-2008-06-27-66. Justis- og beredskapsdepartementet.

En helhetlig integreringspolitikk (2012): Barne-, Likestillings- og Inkluderingsdepartementet. Meld. St. 6 (2012–2013).

Eskeland, Ståle (2006) *Fangerett*. Oslo: Cappelen Akademisk.

Et bedre personvern. Oslo: Statens Forvaltningstjeneste 1997. (Norges offentlige utredninger, NOU 1997:19).

Europa.eu (2009): *The Schengen area and Cooperation*.
URL:http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_en.htm [Lesedato: 7.3.2013].

Europa.eu (2010): *«Eurodac» system.*
URL:http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33081_en.htm [Lesedato: 23.2.2013].

Europa.eu (2011): *Schengen: EU Commission proposes a European approach to better protect citizens' free movement.* URL: http://europa.eu/rapid/press-release_IP-11-1036_en.htm [Lesedato: 28.3.2013].

Europa.eu (2012): *European Information Exchange Model (EIXM).* URL: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/eixm/index_en.htm [Lesedato: 25.3.2013].

Europa.eu (2013): *Treaty of Lisbon. Taking Europe into the 21st century*. URL: http://europa.eu/lisbon_treaty/glance/index_en.htm [Lesedato: 19.3.2013].

European Commission (2011): *Press release: EU 'Smart Borders': Commission wants easier access and enhanced security.* URL: http://europa.eu/rapid/press-release_IP-11-1234_en.htm [Lesedato: 12.3.2013].

European Commission (2012): *Visa Information System (VIS).* URL: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm [Lesedato: 2.3.2013].

European Commission (2013): *Press release: Schengen Information System (SIS II) goes live*. Reference: IP/13/309, 09/04/2013. URL: http://europa.eu/rapid/press-release_IP-13-309_en.htm?locale=en [Lesedato: 11.4.2013].

European Convention on Human Rights. European Court of Human Rights. Council of Europe. Strasbourg.

Europol.europa.eu/ (2013): *About us.* *URL: https://www.europol.europa.eu/content/page/about-us* [Lesedato: 23.2.2013].

Fierke, K.M (2007): *Critical Approaches to International Security*. Cambridge: Polity Press.

Foucault, Michel (1975): *Overvåking og straff.* Oslo: Gyldendal.

Frontex.europa.eu (2012): *Mission and tasks*. URL: http://www.frontex.europa.eu/about/mission-and-tasks. [Lesedato: 10.3.2013].

Holmén, Hans og Magnus Jirström (2009): "Look Who's Talking! Second Thoughts about NGO's as Representing Civil Society" I: *Journal of Asian and African Studies.* SAGE Publications. Vol 44 (4).

Høigård, Cecilie (1997): "Kriminalitetsbilder og kriminalstatistikk" I: *Kriminologi*. Liv Finstad og Cecilie Høigård (red.). Oslo: Pax Forlag.

Inexproject.eu (2013): *Description of The Project*. URL:http://www.inexproject.eu/index.php?option=com_content&view=article&id=50&Itemid=57 [Lesedato: 2.2.2013].

Iso.org (2013): *ISO/IEC 27000:2012*. URL:http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56891 [Lesedato: 2.2.2013].

Johannessen, Asbjørn, Per Arne Tufte og Line Christoffersen (2010): *Introduksjon til samfunnsvitenskapelig metode*. Oslo: Abstrakt Forlag.

Jones, Chris (2012): *"Complex, technologically fraught and expensive" - the problematic implementation of the Prüm Decision.* Statewatch.

Kriminalstatistikk 2000. Oslo-Kongsvinger: Statistisk Sentralbyrå, 2000. (Norges Offisielle Statistikk).

Kriminalstatistikk 2010. Oslo-Kongsvinger: Statistisk Sentralbyrå, 2010. (Norges Offisielle Statistikk).

Kripos (2011): *Varsel om vedtak – tilbakemelding til foreløpig rapport.* Brev fra Kripos til Datatilsynet datert 15.9.2011.

Kvam, Bjarne (2008): *Norge og Schengen: Et svekket samarbeid mot kriminalitet*. Cappelen Akademisk.

Loader, Ian (2002): "Governing European Policing: Some Problems and Prospects, Policing and Society". I: *An International Journal of Research and Policy*. London: Routledge.

Loader, Ian og Neil Walker (2007): *Locating the Public Interest in Transnational Policing. EUI Working Paper LAW No.2007/17.* European University Institute, Department of Law.

Lovdata (2013): *Tigging*. URL: http://www.lovdata.no/nyhet/forside/20130204-soketips.html [Lesedato: 15.4.2013].

Lund, Ketil (2010): " Nedbyggingen av den liberale rettsstat". I: *Til forsvar for personvernet.* John O. Egeland (red.). Oslo: Universitetsforlaget.

Marini, Adelina (2011): *Schengen is for the lighter greens.*
URL: http://www.euinside.eu/en/comments/schengen-is-for-the-lighter-greens [Lesedato: 17.3.2013].

Mathiesen, Thomas (1997): *Schengen: politisamarbeid, overvåking og rettssikkerhet i Europa*. Oslo: Spartacus Forlag.

Mathiesen, Thomas (1997): "The Viewer Society: Michel Foucaults "Panopticon" Revisited" I: *National Security and The Rule of Law.* Tollborg, Dennis (red.). Göteborg: Centrum for Europaforskning.

Mathiesen, Thomas (2000): *Siste ord er ikke sagt. Schengen og globaliseringen av kontroll*. Oslo: Pax Forlag.

Mathiesen, Thomas (2005): *Retten i samfunnet.* Oslo: Pax Forlag.

Mathiesen, Thomas (2008): Lex Vigilatoria: Global control without a state. I: *Surveillance and governance. Crime control and beyond*. Mathieu Deflem (red.). Bingley: Emerald Group Publishing Limited.

Mathiesen, Thomas (2013): *Towards a Surveillant Society. The Rise of Surveillance Systems in Europe.* Utkommer på Waterside Press, 2013. England.

Melgård, Marie (2013): "Blir aldri noen regjering som sier nei til Schengen». I: *Aftenposten*. Onsdag 10.4.2013 s.8.

Mertens, Hans Joachim (1997): "Lex Mercatoria: A self-applying system beyond national law?" I: *Global law without a state.* Gunther Teubner (red.). Darthmouth Publishing Company.

Nrk.no (2013): *Politimesteren i Oslo: Problemet er utlendinger, ikke innvandrere.*
URL: http://www.nrk.no/nyheter/norge/1.10938373 [Lesedato: 10.3.2013].

Ny Offentlighetslov. Oslo: Statens Forvaltningstjeneste 2003. (Norges Offentlige Utredninger, NOU 2003:30).

Parkin, Joanna (2011a): "The Difficult Road to the Schengen Information System II: The legacy of "laboratories" and the cost for fundamental rights and the rule of law". I: *CEPS Paper in Liberty and Security in Europe, April 2011.* Centre for European Policy Studies.

Parkin, Joanna (2011b): "The Schengen Information System and the EU Rule of Law". I: *INEX Policy Brief no.13/June 2011*. International Peace Research Institute Oslo.

Paul, James A. (2000): *NGO's and Global Policy-making.* URL:http://www.globalpolicy.org/component/content/article/177/31611.html [Lesedato: 16.2.2013].

Pearsall, Beth (2010): "Predictive Policing: The Future of Law Enforcement?" I: *National Institute of Justice Journal Issue No. 266.* s.16-19.

Schengenkonvensjonen (IV) (2007). Brussels. Council of The European Union.

Sheptycki, James (1995): "Transnational policing and the makings of a postmodern state". I: *The British Journal of Criminology*. *Vol 35, no.4.*

Sheptycki, James (2007): "High Policing in the Security Control Society". I: *Policing. Volume 1, Number 1* s.70-79. Oxford University Press.

SIS-Loven. Lov om Schengen Informasjonssystem av 16.juni 1999.

Statewatch.org (2012): *EU: Collection of personal data for the EU's Visa Information System spreads further across the globe. URL:* http://database.statewatch.org/article.asp?aid=31887 [Lesedato: 2.3.2013].

Statewatch.org (2013a): *EU: API, PNR, threat assessments, and data-mining: Member States push for access to travellers' personal data for customs authorities.* *URL:* http://database.statewatch.org/article.asp?aid=32147 [Lesedato: 2.3.2013].

Statewatch.org (2013b): *About us.* URL: http://www.statewatch.org/about.htm [Lesedato: 10.2.2013].

Statistisk Sentralbyrå (2012): *Etterforskede Lovbrudd, 2010.* URL: http://www.ssb.no/lovbrudde/ [Lesedato: 10.03.2013].

Stortingsproposisjon nr. 50 (1998/1999). Utenriksdepartementet.

Tamanaha, Brian Z. (2004): *On the rule of law. History, politics, theory.* Cambridge University Press.

Teubner, Gunther (1997): "Global Bukowina: Legal Pluralism in the world society". I: *Global law without a state.* Gunther Teubner (red.). Darthmouth Publishing Company.

The Council of the European Union (2005): "The Hague Programme: Strengthening freedom, security and justice in the European Union". *I: Official Journal of the European Union.*

The Joint Supervisory Authority of Schengen (1996): *Rules of Procedure of The Joint Supervisory Authority.*

The Joint Supervisory Authority of Schengen (2013): *Tasks of the JSA.* URL:http://schengen.consilium.europa.eu/about/tasks-of-the-jsa-schengen.aspx?lang=en [Lesedato: 2.2.2013].

Töpfer, Eric (2011): "Lubricating the flow of information in the EU" I: *Statewatch Journal; vol. 21 no. 1 January-March 2011.*

Udi.no (2013): *Oppholdsrett i Norge for EU/EØS/EFTA-borgere.* URL: http://www.udi.no/Sentrale-tema/Arbeid-og-opphold/Arbeid-og-opphold-EU-EOS-EFTA-borgere/ [Lesedato: 2.3.2013].

Vg.no (2013): *Tigger-registrering kan være lovbrudd*. URL: http://www.vg.no/nyheter/innenriks/artikkel.php?artid=10102180 Verdens Gang 8.4.2013. [Lesedato:8.4.2013].

Vedlegg

Vedlegg 1: Kvittering på innmeldt prosjekt fra Norsk Samfunnsvitenskapelig Datatjeneste.

Vedlegg 2: Informasjonsbrev.

Vedlegg 3: Intervjuguide.

Vedlegg 4: Liste over forkortelser.

Vedlegg 1: Kvittering på innmeldt prosjekt fra Norsk Samfunnsvitenskapelig Datatjeneste

Norsk samfunnsvitenskapelig datatjeneste AS
NORWEGIAN SOCIAL SCIENCE DATA SERVICES

Harald Hårfagres gate 29
N-5007 Bergen
Norway
Tel: +47-55 58 21 17
Fax: +47-55 58 96 50
nsd@nsd.uib.no
www.nsd.uib.no
Org.nr. 985 321 884

Thomas Mathiesen
Institutt for kriminologi og rettssosiologi
Universitetet i Oslo
Postboks 6706 St. Olavs plass
0130 OSLO

Vår dato: 26.01.2012 Vår ref: 29101 / 3 / LT Deres dato: Deres ref:

KVITTERING PÅ MELDING OM BEHANDLING AV PERSONOPPLYSNINGER

Vi viser til melding om behandling av personopplysninger, mottatt 18.12.2011. Meldingen gjelder prosjektet:

29101	*Globalisering, internasjonal overvåking og rettssikkerhet*
Behandlingsansvarlig	*Universitetet i Oslo, ved institusjonens øverste leder*
Daglig ansvarlig	*Thomas Mathiesen*
Student	*Renate Wejset*

Personvernombudet har vurdert prosjektet og finner at behandlingen av personopplysninger er meldepliktig i henhold til personopplysningsloven § 31. Behandlingen tilfredsstiller kravene i personopplysningsloven.

Personvernombudets vurdering forutsetter at prosjektet gjennomføres i tråd med opplysningene gitt i meldeskjemaet, korrespondanse med ombudet, eventuelle kommentarer samt personopplysningsloven/-helseregisterloven med forskrifter. Behandlingen av personopplysninger kan settes i gang.

Det gjøres oppmerksom på at det skal gis ny melding dersom behandlingen endres i forhold til de opplysninger som ligger til grunn for personvernombudets vurdering. Endringsmeldinger gis via et eget skjema, http://www.nsd.uib.no/personvern/forsk_stud/skjema.html. Det skal også gis melding etter tre år dersom prosjektet fortsatt pågår. Meldinger skal skje skriftlig til ombudet.

Personvernombudet har lagt ut opplysninger om prosjektet i en offentlig database, http://www.nsd.uib.no/personvern/prosjektoversikt.jsp.

Personvernombudet vil ved prosjektets avslutning, 31.12.2013, rette en henvendelse angående status for behandlingen av personopplysninger.

Vennlig hilsen

Vigdis Namtvedt Kvalheim

Lis Tenold

Kontaktperson:Lis Tenold tlf: 55 58 33 77
Vedlegg: Prosjektvurdering
Kopi: Renate Wejset, Kirkeveien 50, 0368 OSLO

Vedlegg 2: Informasjonsbrev

Forespørsel om å delta på intervju i forbindelse med en masteroppgave i rettssosiologi

Som masterstudent i rettssosiologi ved Institutt for Kriminologi og Rettssosiologi ved Universitetet i Oslo kontakter jeg med dette skrivet personer som jeg anser som aktuelle informanter i min studie.

Det overordnede temaet for mitt prosjekt er *globalisering, internasjonal overvåking og rettssikkerhet.* Jeg ønsker å belyse dette ved å komme i kontakt med personer/instanser med ulik tilknytning til feltet.

Jeg ønsker å foreta et kvalitativt intervju med deg som utvalgt. Intervjuet vil ta maksimalt en time og vi blir sammen enige om passende tid/sted. Jeg vil under intervjuet benytte båndopptaker og ta notater.

Det er frivillig å delta og du har mulighet til å trekke deg når som helst underveis, uten å måtte begrunne dette nærmere. Dersom du trekker deg vil alle innsamlede data om deg bli slettet. Opplysningene vil bli behandlet konfidensielt, og ingen enkeltpersoner vil kunne gjenkjennes i den ferdige oppgaven. Opplysningene anonymiseres og opptakene slettes når avhandlingen er ferdig skrevet, innen utgangen av 2013.

Jeg vil sette stor pris på om du har anledning til å stille til intervju - dersom det er aktuelt er det fint om du skriver under på den vedlagte samtykkeerklæringen og sender den til meg.

Hvis det er noe du lurer på kan du ringe meg på 47 83 50 95, eller sende en e-post til renatewe@student.jus.uio.no. Du kan også kontakte min veileder Professor Thomas Mathiesen ved institutt for Kriminologi og rettssosiologi på telefonnummer 22 85 01 16.

Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste (NSD).

Med vennlig hilsen
Renate Wejset
Kirkeveien 50
0368 Oslo

Samtykkeerklæring:

Jeg har mottatt informasjon om studien av internasjonal overvåking og rettssikkerhet og ønsker å stille på intervju.

Signatur …… Telefonnummer …

Vedlegg 3: Intervjuguide

Intervjuguide

- Informasjon til samtlige informanter:

(Jeg gir en overordnet innføring i prosjektet).

Jeg vil gjøre oppmerksom på at dine svar ikke vil kunne spores tilbake til deg i avhandlingen. Du kan si i fra om det er spørsmål du ikke ønsker å svare på, og du kan når som helst trekke deg under intervjuet.

Spørsmål til samtlige informanter (intervjuer på norsk):

Generelt:

1) Er det ok om jeg benytter båndopptaker under intervjuet?
2) Ønsker du å være anonym, eller kan ditt navn nevnes i avhandlingen?
3) Kan du/dere fortelle litt om din/deres faglige bakgrunn?

Generelt om Schengen/Schengen Informasjonssystem:

1) I hvilken grad vil du si du har kjennskap til Schengen og SIS (Schengen Informasjonssystem)?
2) Hvilke tanker har du rundt rettssikkerhet og personvern i forbindelse med Schengen og overvåkingssystemene sett fra ditt ståsted?
3) Har du noen tanker om hva slags effekt Schengen og disse systemene har på kriminalitetsbildet i Europa?
4) Har du forslag til hva som kan gjøres for å bedre rettssikkerheten i systemene?
5) Hvorfor tror du denne problematikken ikke er mer på dagsorden i media og blant folk flest?
6) Kontrollen med systemene – er den god nok?
7) Vi må innrette oss etter regler på et overnasjonalt nivå – hvilke tanker har du rundt dette?
8) Hvordan tror du systemene og overvåkingen generelt kommer til å utvikle seg i fremtiden?
9) Er det noe du vil påpeke til slutt som er viktig å få med angående dette temaet?

Spørsmål til Datatilsynet

1) Kan du fortelle litt om Tilsynsavdelingen – hvor mange ansatte er dere, deres oppgaver osv.?
2) Hvilke oppgaver har Datatilsynet (Tilsynsavdelingen) overfor Kripos? Spesielt SIS?
3) Hvor ofte/i hvilken grad er dere i kontakt med Kripos?
4) Hva ser dere etter når dere er på tilsyn?
5) Hvordan stiller Datatilsynet seg generelt til Schengen?
6) Hva kan gjøres i systemene for å forbedre disse?
7) Når dere fører kontroll – hva måler dere opp mot?
8) Kan du fortelle litt rundt rollen Datatilsynet hadde i tiden da overvåkingssystemene i Schengen ble rullet ut for fullt?
9) Hadde dere tett samarbeid/kontakt med Kripos i denne tiden?
10) Hvordan vil du si Datatilsynets syn på dette var med hensyn til rettssikkerhet?
11) Norge har Datatilsynet – har du noe inntrykk av hvordan situasjonen er i andre land?
12) Hva mener du blir de viktigste oppgavene for Datatilsynet i årene som kommer?
13) Kan du fortelle litt om foreningen *Digitalt Personvern*?

Aktuelle punkter:

- Datalagringsdirektivet (til sammenlikning).

Spørsmål til andre informanter:

1) Samfunnsvernet veier tyngre enn personvernet skriver du i ”Nedbyggingen av den liberale rettsstat” – kan du utdype dette?
2) Lundkommisjonen – granskning av politiets overvåkingstjeneste. Kan noen av erfaringene/oppdagelsene fra den gang også brukes i dag? Ser du noen likhetstrekk/har noe forandret seg?

Aktuelle punkter: ICJ (International Commission of Jurists).

Spørsmål til KRIPOS:

1) Hva er din stillingsbetegnelse og hvilke oppgaver har du?
2) I hvilken grad er du i kontakt med andre nasjoner i ditt arbeide? Hvordan synes du samarbeidet fungerer?
3) Kan du si noe om hvordan kommunikasjonen foregår og hvordan denne fungerer?
4) Det er mellom landene noe ulik praksis. Er dette noe som kan skape utfordringer i det daglige arbeidet? Er det iverksatt tiltak for å bedre situasjonen?
5) Er det rom for bruk av skjønn i systemene?

6) Når det gjelder informasjons- og overvåkingssystemene i Schengen – i hvilken grad vil du fra ditt ståsted si at rettssikkerheten er ivaretatt?
7) Hvordan fungerer etter din mening European Data Protection Supervisor (EDPS)?

Interview guide – European Data Protection Supervisor

These are the questions that I would like the EDPS to answer. If there are any of the questions you do not wish to answer please let me be notified.

1) Can you please tell me in what way the EDPS is organized? Where are you situated, how large is the organization and so on?
2) What is the main goal for EDPS?
3) In what way do you look after the systems and keep control with all the countries involved?
4) There are some critical voices aimed at systems like SIS and SIRENE – in what way do you think this is justified?
5) What is the EDPS's opinion regarding the rule of law in the registration/surveillance systems?
6) There is a review of the EU framework for data protection – can you tell me about this? Is a new directive on its way?
7) What do you regard as the largest challenges the EDPS is having today and will have in the future?
8) What do you think needs to be done to improve the systems and its security?
9) Do you have any thoughts on what effect Schengen and its systems has on the crime in Europe?
10) How do you think the registration- and surveillance structure in Europe will develop in the future?
11) Finally; is there anything you would like to point out that you think is important in this matter?

Interview guide - Statewatch

Would you like to stay anonymous, or can I mention that I have spoken to you in my assignment?

1) Can you please tell me about your organization Statewatch? How you are organized? What is your background? How many people are you?
2) What is your main goal? And how do you work?

(My main interest is Schengen and the Schengen information system (SIS.)

3) In your opinion; what effect do these systems (and Schengen) have in Europe? For example regarding crime?
4) What is your opinion when it comes to these systems in Europe regarding the rule of law and privacy? – are the control with the systems good enough? Do you have any suggestions on what can be done to improve the systems regarding the rule of law?
5) In Norway; this subject is very rarely mentioned in the media – I don't know how it is in the UK. What do you think is the reason for the medias lack of interest?
6) How do you think the so called *surveillance society* will develop in the future?
7) Do you have any suggestions on what can be done to improve the systems regarding the rule of law and so on?

Vedlegg 4: Liste over forkortelser

CEPOL – European Police College

EDPS – European Data Protection Supervisor

EFTA – European Free Trade Association

EØS – Det Europeiske Økonomiske Samarbeidsområdet

ICJ – International Commission of Jurists

JSA – Joint Supervisory Authority of Schengen

NGO – Non-governmental Organization

PNR – Passenger Name Record

SIRENE – Supplementary Information Request of the National Entries

SIS – Schengen Informasjonssystem

VIS – Visa Information System

Antall ord: 42755